La Bibliothèque de menaces est une base de connaissances de techniques répressives, de mesures d'atténuation qui peuvent être prises pour les contrer, et d'opérations répressives où elles ont été utilisées. Le but est d'aider les anarchistes et autres rebelles à comprendre les options à la disposition de leurs adversaires, développer des modèles de menaces adaptés, et au final réussir dans leurs actions et projets.

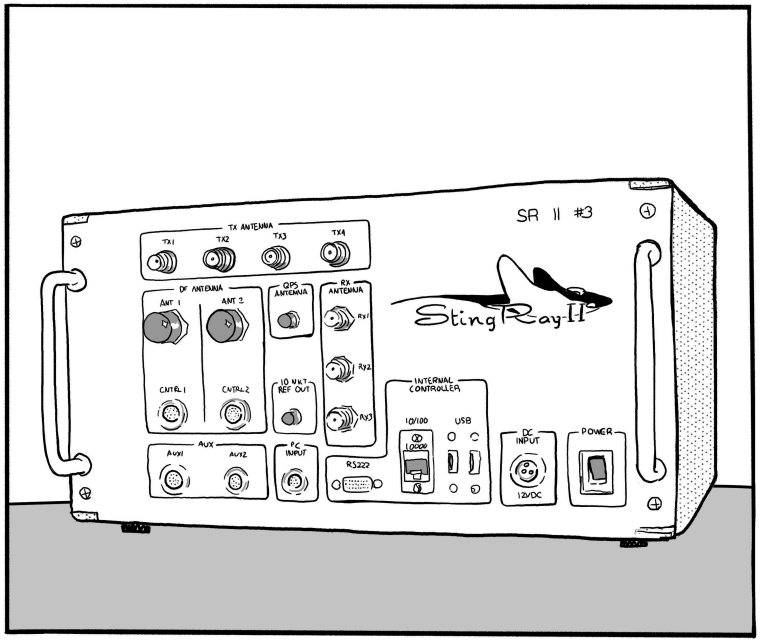
No Trace Project / Pas de trace, pas de procès. Un ensemble d'outils pour aider les anarchistes et autres rebelles à **comprendre** les capacités de leurs ennemis, **saper** les efforts de surveillance, et au final **agir** sans se faire attraper.

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.

Bibliothèque de menaces

Partie 3/5

Techniques Su–V



4 novembre 2025

Un résumé des mises à jour depuis cette date est disponible sur : notrace.how/threat-library/fr/changelog.html

Cette brochure est divisée en plusieurs parties. Les chapitres dans la partie actuelle sont référencés par leurs numéros de page. Les chapitres dans d'autres parties sont référencés par le symbole # suivi du numéro de la partie.

Texte d'origine en français

No Trace Project

notrace.how/threat-library/fr

Mesures d'atténuation

Cachette ou planque (#4) : Tu peux garder du matériel d'action qui n'a pas de fonction « légitime » dans une cachette ou une planque, ou, au pire, le laisser transiter chez toi seulement pendant très peu de temps.

Clandestinité (#4) : Si tu entres en clandestinité, un adversaire ne peut pas savoir où tu vis, et ne peut donc pas faire une visite discrète de ton domicile.

Détection d'intrusion physique (#4) : Tu peux prendre des mesures de détection d'intrusion physique pour détecter une visite discrète de domicile.

Se préparer aux perquisitions (#4) : Tu peux te préparer pour une visite discrète de domicile en minimisant la présence d'objets qui pourraient être problématiques en cas de visite.

Opérations répressives

Répression contre Zündlumpen (#5) : Les enquêteurs ont fait une visite discrète des cabanes où vivaient N. et M. pour y prélever des **échantillons d'odeur (#1)**.[17]

Opération contre Peppy et Krystal (#5) : Les enquêteurs ont secrètement fouillé la poubelle devant le domicile de Peppy et Krystal, où ils ont trouvé des documents suspects.[22]

Opération contre Direct Action (#5) : Après avoir entendu (vraisemblablement pendant une opération de **surveillance physique (p. 26)**) que quatre membres de Direct Action qui vivaient ensemble dans une maison allaient quitter la maison pendant deux jours pour faire du camping, les enquêteurs ont fait deux visites discrètes de la maison sur ces deux jours :[9]

- Le premier jour, ils ont visité la maison pour y trouver un bon endroit pour installer des microphones cachés le jour suivant et pour repérer d'éventuels pièges.
- Le deuxième jour, ils ont visité la maison pour y installer des microphones cachés et prendre des photos d'objets et documents suspects.

La torture comprenait :[88]

Répression du soulèvement de 2019 au Chili (#5) : Dans les rues et en garde-à-vue, les policiers et soldats ont blessé, agressé sexuellement, violé, torturé et tué de nombreuses manifestant·e·s, vraisemblablement dans une volonté stratégique de dissuader les manifestant·e·s de participer au soulèvement.[63]

3.27. Visite discrète de domicile

Utilisée par la tactique : **Incrimination**

Une visite discrète de domicile est une visite secrète d'une résidence effectuée par un adversaire lorsque les occupant·e·s ne sont pas présents.

Un adversaire peut faire une visite discrète de domicile pour :

- Rassembler des informations.
- Cacher des **dispositifs de surveillance (#1)** dans le domicile.
- Installer des **malware (p. 22)** sur des appareils numériques.

Généralement, quand un adversaire fait une visite discrète d'un domicile, il ne veut pas que les occupant·e·s sachent que l'opération a eu lieu. Ainsi, en général :

- Si le domicile a des portes verrouillées, l'adversaire doit passer les portes sans les abîmer de manière visible. Il peut faire ça en crochetant la serrure ou en demandant les clés au propriétaire du bâtiment.
- L'adversaire s'abstient de saisir des objets ou de bouger des choses.

En plus de visiter le domicile, l'adversaire peut saisir discrètement les poubelles à l'extérieur du domicile dans l'espoir d'y trouver des informations intéressantes (par exemple des notes écrites ou des preuves forensiques comme des traces ADN).

88· des tabassages et des décharges électriques.

Sommaire

3. Techniques

3.19. Surveillance de masse

Utilisée par les tactiques : **Dissuasion**, **Incrimination**

La surveillance de masse est la surveillance à grande échelle de la totalité ou d'une partie substantielle d'une population. C'est la surveillance de fond de notre société.

3.19.1. Fichiers de police

Les fichiers de police sont des dossiers physiques ou numériques produits par des agences de maintien de l'ordre. Les fichiers de police contiennent de grandes quantités d'informations à propos de beaucoup de choses, sont conservés indéfiniment ou pour de longues périodes, et peuvent être efficacement analysés et croisés grâce à des outils numériques.

Voici des exemples notables de fichiers de police :

- Les bases de données de documents d'identité officiels (cartes d'identité, permis de conduire, passeports).
- Les bases de données d'informations biométriques (photos de visages, empreintes digitales, ADN).
- L'historique des **vérifications d'identité (p. 40)**, amendes, arrestations, enquêtes, procédures judiciaires, et condamnations.

Mesures d'atténuation

Attaque (#4) : Tu peux détruire les armoires qui stockent les fichiers de police papier et les data centers qui stockent les fichiers de police numériques.

- Protéger les personnes encore libres, au cas où la personne arrêtée « parle ». Cela va dépendre de ce que sait la personne arrêtée, et peut inclure abandonner des **planques (#4)**, interrompre des projets, entrer en **clandestinité (#4)**, etc.
- Vous préparer psychologiquement à résister à la torture.

Voir « Under the Enemy's Blade: A Search for Anarchist Practices Against Torture »[84] (*Sous la lame de l'ennemi : À la recherche de pratiques anarchistes contre la torture*) à propos de pratiques contre la torture.

Opérations répressives

Network (#5) : La plupart des accusé·e·s ont été torturé·e·s par le Service fédéral de sécurité de la fédération de Russie (FSB) au début de leurs détentions pour obtenir des déclarations (souvent falsifiées) qui pourraient ensuite être utilisées pour les incriminer et les condamner.[85] La plupart des accusé·e·s qui ont été torturé·e·s ont plus tard renié leurs déclarations et dénoncé publiquement la torture qui leur a été infligée.

Renata (#5) : Pendant une perquisition, une des personnes arrêté·e·s a été forcée de se mettre à genoux par un policier qui a pointé un pistolet contre sa tempe.[86]

Opération contre Amos Mbedzi (#5) : Mbedzi a été torturé dans les premiers jours de sa détention.[7]

Partisans anarchistes biélorusses (#5) : Les personnes ont été torturées dans les premiers jours de leur détention.[87]

Les trois de Varsovie (#5) : Les personnes ont été torturées pendant leur arrestation et les premières heures de leur détention.[77]

Opération contre Ruslan Siddiqi (#5) : Ruslan Siddiqi a été torturé pendant plusieurs jours après son arrestation.[78] Sous la torture, il a avoué avoir mené l'attaque à l'explosif contre le train et l'attaque contre l'aérodrome militaire.

[85] https://web.archive.org/web/20210724133854/https://a2day.net/network-underground

[86] https://infernourbano.altervista.org/che-si-sappia-comunicato-dal-trentino

[87] https://pramen.io/en/2021/12/blood-on-your-hands-regarding-information-about-torture-of-anarcho-partisans

Dans certains contextes, la violence physique peut inclure de la torture. Par exemple, en Russie et Biélorussie, plusieurs anarchistes ont été torturés ces dernières années après avoir été arrêtés par l'État. Les actes de tortures constatés dans ces pays incluent :[83]

Dans certains contextes, la violence physique peut inclure des assassinats.

Mesures d'atténuation

Principe du *need-to-know* (#4) : Si toi, ou des membres de ton réseau, risquez d'être torturé·e·s par un adversaire, vous pouvez appliquer le principe du *need-to-know* pour que chaque personne connaisse le moins d'informations sensibles possible et donc ait le moins d'informations possible à fournir aux tortionnaires.

Voir « Under the Enemy's Blade: A Search for Anarchist Practices Against Torture »[84] (*Sous la lame de l'ennemi : À la recherche de pratiques anarchistes contre la torture*) à propos de pratiques contre la torture.

Se préparer à la répression (#4) : Si toi, ou des membres de ton réseau, risquez d'être torturé·e·s par un adversaire, vous pouvez vous préparer à ce risque. Par exemple, vous pouvez :

- Mettre en place des protocoles de communication qui permettent d'apprendre le plus rapidement possible lorsqu'une personne est arrêtée afin de prendre des mesures immédiates pour :
  - Protéger la personne arrêtée. Dans certains contextes où la torture se limite aux premières heures ou premiers jours de la détention, exercer de la pression sur l'adversaire aussi vite que possible après l'arrestation (par exemple en impliquant des avocats ou des journalistes) peut aider à arrêter la torture ou limiter la sévérité des actes de torture.

83

des tabassages, la suffocation avec un sac en plastique ou un oreiller, de l'eau versée dans le nez et la bouche, la suspension par les jambes ou par les mains, des décharges électriques, la torture avec un tourne-vis, forcer des personnes à faire des squats jusqu'à ce qu'elles s'écroulent, des violences sexuelles, et la privation de sommeil, de nourriture et d'eau.

84 https://notrace.how/resources/fr/#under-enemy-blade

Opérations répressives

Opération contre Boris (#5) : Les enquêteurs ont découvert que l'ADN sur le bouchon de bouteille appartenait à Boris car son ADN était présent dans le Fichier national automatisé des empreintes génétiques (FNAEG).[1]

Les enquêteurs ont obtenu et analysé l'historique de l'activité de la police locale (contrôles d'identité et amendes) peu de temps avant et après les sabotages, dans différents périmètres autour de là où les sabotages ont eu lieu, en espérant vraisemblablement trouver les noms des saboteurs dans cet historique.

Opération de 2011-2013 contre Jeremy Hammond (#5) : Sous son identité numérique, Jeremy Hammond a partagé lors des conversations en ligne qu'il avait été arrêté à l'édition 2004 de la convention du parti républicain, était passé par une prison fédérale et une prison de comté, et était actuellement sous contrôle judiciaire.[2] Les enquêteurs ont pu vérifier tout cela grâce à des fichiers de police, ce qui les a aidé à relier l'identité numérique de Jeremy Hammond à son identité réelle.

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont amplement utilisé des fichiers de police pour faire des liens entre des gens, dont le Fichier national des permis de conduire, le Fichier des véhicules assurés, ainsi que les fichiers d'arrestations, de procédures judiciaires et de condamnations.[3]

3.19.2. Mouchards civils

Les mouchards civils sont des personnes qui ne font pas partie des forces de sécurité d'un adversaire, mais qui préviendraient l'adversaire s'ils observaient quelque chose de suspect.

Par exemple, un mouchard civil qui est témoin d'un crime et qui s'identifie à l'État va probablement appeler la police, fournir une description du ou des suspects, et pourrait même suivre les suspects jusqu'à ce que la police intervienne ou témoigner dans le cadre d'une enquête criminelle.

1 https://rupture.noblogs.org/post/2023/10/04/no-bars

2 https://notrace.how/documentation/jeremy-hammond-affidavit.pdf

3 Source non publique.

Mesures d'atténuation

Attaque (#4) : Si un civil te suit après une action, tu peux lui faire peur avec des menaces ou du spray au poivre. Si un civil essaie d'appeler la police, tu peux détruire son téléphone.

Préparation minutieuse de l'action (#4) : Les civils peuvent t'observer pendant une action et transmettre leurs observations à un adversaire. Pour contrer ça, tu peux mener les actions la nuit ou dans des zones peu fréquentées pour minimiser les témoins, et utiliser un·e guetteu·r·se pour être avertit de la présence de témoins dès qu'ils sont repérés. Fais attention aux balcons et fenêtres surplombant le lieu de l'action.

Tenue anonyme (#4) : Tu peux porter une tenue anonyme pour empêcher les civils de fournir une description de toi qui serait utile à un adversaire.

Opérations répressives

Fenix (#5) : Quand Lukáš Borl était en clandestinité, sa photo et ses informations personnelles ont été publiées sur le site web de la police nationale pour encourager les citoyens à envoyer à la police des informations à son propos.[4]

Opération de 2019-2020 contre Mónica et Francisco (#5) : La vendeuse du magasin de téléphones portables où Mónica a acheté un téléphone qui a été utilisé dans l'action de 2020, interrogée par les enquêteurs, a donné une description d'une personne qui, selon les enquêteurs, correspondait à Mónica.[5]

Arrestation de Stecco (#5) : Après avoir arrêté Stecco les enquêteurs ont montré sa photo à de nombreuses personnes vivant près du lieu de l'arrestation et leur ont posé des questions, ce qui leur a permis de trouver la maison où Stecco aurait vécu.[6]

Opération contre Amos Mbedzi (#5) : Lorsque l'engin explosif a explosé prématurément et blessé gravement Mbedzi, un civil circulait en voiture

[4]https://antifenix.noblogs.org/post/2016/03/11/confirmed-lukas-borl-under-police-investigation

[5]https://notrace.how/resources/fr/#monica-francisco

[6]https://notrace.how/resources/fr/#cose-utili-da-sapere

Les vigiles (aussi connus sous le nom d'*agents de sécurité*) sont des personnes employées par un adversaire pour protéger des bâtiments ou autres infrastructures physiques.

Si des vigiles détectent une présence non autorisée dans la zone qu'ils surveillent, ils peuvent décider d'intervenir eux-mêmes ou d'appeler à l'aide. En fonction du contexte, ils peuvent être équipés d'armes léthales ou non-léthales.

Mesures d'atténuation

Attaque (#4) : Avant ou pendant une action, tu peux immobiliser des vigiles pour les empêcher t'interférer avec l'action. Par exemple, dans leurs actions contre les machines d'entreprises d'exploitation forestière sur le territoire contrôlé par l'État chilien, des Mapuches ont neutralisé des vigiles en les désarmant,[80] en les ligotant[81] ou en leur tirant dessus.[82]

Reconnaissance (#4) : Avant une action, tu peux déterminer si des vigiles sont présents sur le lieu de l'action.

Opérations répressives

Opération contre Louna (#5) : Dans les jours précédant l'incendie, un vigile a vu des véhicules suspects circuler près du lieu de l'incendie, les a pris en photo, et, après l'incendie, a fourni les photos aux enquêteurs.[3]

3.26. Violence physique

Utilisée par les tactiques : **Dissuasion**, **Incrimination**

La violence physique est l'utilisation de la force physique par un adversaire pour intimider une cible ou son réseau, empêcher une cible de poursuivre ses activités, ou contraindre une cible à révéler des informations.

[80]https://actforfree.noblogs.org/post/2022/08/04/chile-a-fiery-july-in-the-mapuche-territories

[81]https://actforfree.noblogs.org/post/2022/02/28/chile-the-mapuche-struggle-continues-under-a-state-of-emergency

[82]https://actforfree.noblogs.org/post/2021/07/21/chile-mapuche-zone-ignites-after-the-murder-of-pablo-marchant-update

Mesures d'atténuation

Fausse identité (#4) : Pendant une vérification d'identité, si fournir ton identité réelle pourrait mener à ton arrestation ou d'autres conséquences négatives, tu peux présenter une fausse identité (tant que la fausse identité n'est pas reconnue comme telle par l'État).

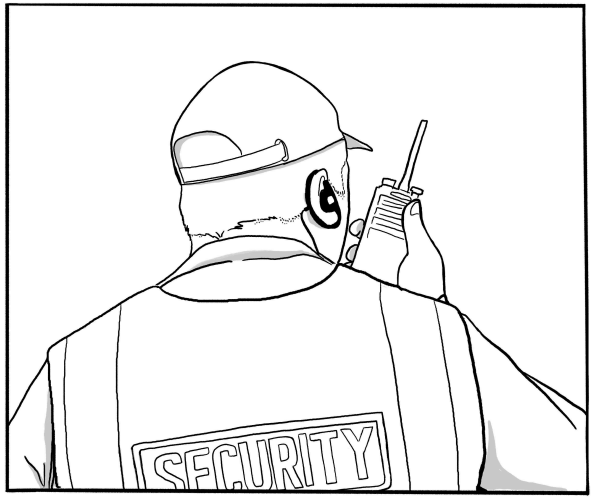
Éviter l'auto-incrimination (#4) : Si possible, tu peux éviter de répondre à des questions ou de fournir tes informations biométriques (photo du visage, empreintes digitales, ADN) pendant une vérification d'identité.

Opérations répressives

Opération contre Boris (#5) : Les enquêteurs ont obtenu et analysé l'historique des contrôles d'identité faits par la police peu de temps avant et après les sabotages, dans différents périmètres autour de là où les sabotages ont eu lieu, en espérant vraisemblablement trouver les noms des saboteurs dans cet historique.[1]

3.25. Vigiles

Utilisée par la tactique : **Arrestation**



sur une route voisine.[7] Le civil s'est arrêté près du lieu de l'explosion, a vu une autre voiture s'arrêter, et a vu Mbedzi crier « Hôpital ! Hôpital ! » et monter dans l'autre voiture. Le civil est resté sur place et a informé les premiers flics qui sont arrivés qu'un homme blessé dans l'explosion était monté dans une voiture vers un hôpital. Cela a vraisemblablement mené à l'arrestation de Mbedzi à l'hôpital une heure plus tard.

De plus, trois civils ont fourni aux enquêteurs des descriptions physiques de Mbedzi : le civil susmentionné, le conducteur de la voiture qui a conduit Mbedzi à l'hôpital et l'agent de sécurité de l'hôpital. Cela a aidé les enquêteurs à reconstituer les déplacements de Mbedzi et à prouver qu'il se trouvait sur le lieu de l'explosion.

Opération contre Louna (#5) : Plusieurs civils ont aidé les enquêteurs. Notamment :[3]

- Après avoir entendu Louna prendre rendez-vous avec un médecin via une écoute téléphonique, les enquêteurs ont contacté le médecin qui a fourni des informations personnelles de Louna, y compris son adresse et son numéro de téléphone.
- La pharmacienne d'une pharmacie où Louna obtenait des médicaments a fourni une description physique de Louna, a affirmé la reconnaître sur une photo, et a fourni des documents personnels de Louna, y compris des copies d'ordonnances.
- Le chef d'établissement d'un établissement d'enseignement supérieur où étudiait une personne a fourni l'emploi du temps de la personne et des informations sur le moyen de transport qu'elle utilisait pour se rendre à l'établissement.

Partisans anarchistes biélorusses (#5) : En tentant de traverser la frontière entre la Biélorussie et l'Ukraine, les personnes se sont arrêtées à un magasin à environ 10 kilomètres de la frontière.[3] Un·e employé·e les a dénoncé aux gardes-frontière, ce qui a directement mené à leur arrestation.

Opération contre Ruslan Siddiqi (#5) : Dans les semaines qui ont suivi l'attaque à l'explosif contre le train, les enquêteurs ont interrogé de nombreux citoyens dans une vaste zone autour du site de l'attaque.[8]

[7] https://notrace.how/documentation/case-against-amos-mbedzi-case-file.pdf
[8] https://theins.ru/en/society/280988

En particulier, les enquêteurs ont interrogé une employée de magasin dans un village. L'employée a dit aux enquêteurs que, avant l'attaque, une personne portant une veste de camouflage et un sac à dos était passée par le magasin. L'employée a fourni une description de la personne, que les enquêteurs ont utilisée pour dresser un portrait-robot. Trois semaines après l'attaque, Ruslan Siddiqi a croisé un flic local qui l'a comparé avec le portrait-robot et l'a arrêté.

Opération contre Direct Action (#5) : Plusieurs civils ont aidé les enquêteurs.[9] Notamment :

- Des journalistes ont dit aux enquêteurs qu'ils avaient remarqué des similitudes entre des communiqués de revendication publiés par Direct Action et des articles d'une publication trimestrielle locale nommée Resistance.
- Un chasseur a, vraisemblablement par hasard, découvert les deux structures en bois dans lesquelles des membres de Direct Action stockaient les explosifs volés qu'iels utilisaient dans des attaques à l'explosif, et a prévenu la police de sa découverte.[10]
- Les propriétaires de la maison où vivaient quatre membres de Direct Action ont donné aux enquêteurs la clé de la maison pour qu'ils puissent y entrer et y installer des microphones cachés.

[9] https://archive.org/details/direct-action-memoirsofan-urban-guerrilla

[10] https://web.archive.org/web/20100715145801/http://uniset.ca/other/cs5/27CCC3d142.html

mes réponses, et [la personne en civil] qui posait les questions a réalisé que je cachais quelque chose. »

Affaire du 8 décembre (#5) : En interrogeant les inculpé·e·s en garde-à-vue, les enquêteurs ont :[79]

- Prétendu que les inculpé·e·s ne seraient pas poursuivis s'ils dénonçaient les autres inculpé·e·s, ce qui était un mensonge.
- Menacé un·e des inculpé·e·s d'agression sexuelle.

3.24. Vérifications d'identité

Utilisée par les tactiques : **Arrestation**, **Incrimination**

Une vérification d'identité est le processus par lequel l'État vérifie l'identité d'une personne en lui demandant ses informations personnelles, en lui demandant de présenter un document d'identité officiel, ou en collectant ses informations biométriques (photo du visage, empreintes digitales, ADN) et en les comparant avec une base de données. Une vérification d'identité peut être un prétexte pour un interrogatoire et des pressions, et peut être suivi d'une fouille des affaires de la personne.

Se soumettre à un contrôle d'identité donne à l'État des informations à ton propos, ce qui peut l'aider à **cartographier ton réseau (#1)**, et peut mener à ton arrestation si il te recherche. Les conséquences d'un refus ou d'une incapacité à se soumettre à un contrôle d'identité dépendent fortement du contexte, mais peuvent inclure avoir tes informations biométriques collectées de force ou à ton insu, être détenu, et être expulsé hors du pays.

La probabilité d'être ciblé par un contrôle d'identité dépend de la situation et de comment tu es perçu·e par l'État. Il est moins probable que tu sois ciblé·e si tu ne fais rien de remarquable et que tu es habillé·e comme un·e bourgeois·e. Il est plus probable que tu sois ciblé·e si tu es perçu·e comme un·e potentiel·le criminel·le ou migrant·e illégal·le, ou si tu es en train de rejoindre ou de quitter une émeute.

[79] https://web.archive.org/web/20250615210912/https://soutien812.blackblogs.org/wp-content/uploads/sites/1922/2023/11/CompteRenduProces_A4.pdf

Mesures d'atténuation

Éviter l'auto-incrimination (#4) : Tu ne devrais en aucun cas parler à un adversaire : c'est le meilleur moyen de résister à ses techniques d'interrogatoire.

Opérations répressives

Opération contre Boris (#5) : En interrogeant des personnes proches de Boris, les enquêteurs ont utilisé des mensonges élaborés pour essayer de les faire parler.[1] Par exemple, les enquêteurs suspectaient vaguement que les personnes interrogées avaient hébergé Boris en avril 2020 et voulaient confirmer leurs suspicions, et ont donc demandé, « Il ressort de nos investigations que vous avez hébergé [Boris] en avril 2020. Combien de temps l'avez vous hébergé ? »

Les trois de Varsovie (#5) : Quelques semaines après le début de sa détention, une personne a donné un témoignage « conséquent » à la police. Il a affirmé que c'était en partie à cause de deux techniques utilisées par l'un·e de ses avocats pour le pousser à donner ce témoignage :[77]

- L'avocat lui a montré une publication sur un réseau social rédigée par une personne de son milieu politique peu après son arrestation. La publication critiquait l'action pour laquelle il a été arrêté et n'incluait pas de déclaration de solidarité. Comme cette publication était la seule réaction en provenance de son milieu politique dont la personne a eu connaissance, il s'est senti isolé.
- L'avocat lui a dit que deux autres personnes avaient déjà donné des témoignages conséquents à la police, ce qui était un mensonge.

Opération contre Ruslan Siddiqi (#5) : Après son arrestation, les enquêteurs n'étaient pas sûrs de l'implication de Ruslan Siddiqi dans l'attaque à l'explosif contre le train.[78] Ils l'ont interrogé et ont déduit qu'il cachait quelque chose. Ruslan Siddiqi raconte : « Ils ont commencé à poser diverses questions sur ce que je faisais [le jour de l'attaque]. J'ai fait des gaffes dans

[77] https://wawa3.noblogs.org/post/2017/05/24/olsen-gang-replies-statements-of-warsaw-three-en

[78] https://danslabrume.noblogs.org/post/2025/03/11/rouslan-sidiki-raconte

3.19.3. Surveillance numérique de masse

Le Utah Data Center (UDC), un centre de stockage de données géant dans l'Utah, aux États-Unis, utilisé pour des activités de surveillance numérique de masse par les agences de renseignement des États-Unis.

La surveillance numérique de masse est la collecte, le stockage, et l'analyse à grande échelle des communications numériques de la totalité ou d'une partie substantielle d'une population.

La surveillance numérique de masse repose sur la collecte de données depuis diverses sources : transactions financières, contrôles aux frontières, pistage GPS des smartphones, et même lampadaires « intelligents ». Les avancées technologiques en capacité de stockage permettent à de vastes quantités de données d'être stockées dans des centres de stockage gérés par l'État. Les avancées technologiques en puissance de calcul permettent l'analyse automatique de ces données pour faciliter le travail des agences de police et de renseignement à l'échelle mondiale.

Voir le sujet « Surveillance numérique ».[11]

Mesures d'atténuation

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques pour rendre la surveillance numérique de masse inefficace. Par exemple, tu peux utiliser Tor[12] pour anonymiser tes activités Internet et tu peux utiliser des systèmes d'exploitation axés sur la sécurité et des

[11] https://notrace.how/resources/fr/#topic=digital-surveillance

[12] https://torproject.org/fr

applications qui limitent les données qu'elles stockent ou collectent à propos de toi.

Chiffrement (#4) : Tu peux chiffrer des données « en mouvement » pour empêcher des observateurs à certains endroits du réseau d'analyser ces données.

Éviter l'auto-incrimination (#4) : Un adversaire peut utiliser la surveillance numérique de masse pour extraire des informations auto-incriminantes d'un appareil numérique. Pour contrer ça, tu peux éviter de stocker de telles informations sur des appareils numériques à part pour des raisons mûrement réfléchies (par exemple écrire et envoyer un communiqué de revendication tout en adoptant de **bonnes pratiques numériques (#4)**).

3.19.4. Vidéosurveillance

La vidéosurveillance de masse est la collecte, le stockage, et l'analyse à grande échelle des données vidéo et audio de caméras de vidéosurveillance. La vidéosurveillance de masse vise à capturer l'identité des personnes qui traversent un espace et à étendre sa couverture autant que possible. Certains pays ont désormais plus de caméras de vidéosurveillance que d'habitants.

Collecte

Voici des sources d'images de vidéosurveillance :

- Les caméras dans la rue ou autres espaces publics.
- Les caméras dans des bâtiments privés (par exemple des magasins, des bureaux).
- Les caméras dans les transports en commun comme les bus, les trains, les autoroutes, etc.
- Les caméras-sonnettes comme Amazon Ring.
- Les caméras intégrées à des véhicules comme sur les Tesla.

Les caméras de vidéosurveillance peuvent grandement varier en qualité, portée, capacités à voir la nuit, présence de microphones, etc.

Mesures d'atténuation

Attaque (#4) : Tu peux attaquer des systèmes d'alarme ou les lignes de communication qu'ils utilisent pour envoyer des signaux d'alerte. Par exemple, tu peux détruire des systèmes d'alarme ou brouiller les signaux d'alerte avec un dispositif de brouillage.

Certains systèmes d'alarme fonctionnent en envoyant des signaux périodiquement ou en continu, même si rien d'anormal n'est détecté. Dans de tels cas, si tu attaques un système d'alarme de telle manière que ses signaux sont interrompus, cela pourrait être interprété comme une alerte et déclencher une intervention.

Bonnes pratiques numériques (#4) : Quand tu effectues une cyber-action, tu peux utiliser des techniques d'évasion numérique[75] pour empêcher les systèmes de détection d'intrusion de détecter l'action.

Reconnaissance (#4) : Avant une action, tu peux inspecter le bâtiment ou l'infrastructure ciblé pour évaluer la présence ou l'absence de systèmes d'alarme, et le type et l'emplacement des capteurs et autres dispositifs d'alarme.

3.23. Techniques d'interrogatoire

Utilisée par la tactique : **Incrimination**

Les techniques d'interrogatoire sont les méthodes utilisées par un adversaire pour obtenir des informations en interrogeant des gens.

Les techniques d'interrogatoire peuvent inclure le mensonge, les menaces, inspirer de la culpabilité, de la honte ou de la fierté, essayer d'apparaître amical et aimable ou, au contraire, menaçant et violent, etc. Dans certains cas, elles peuvent inclure de la **violence physique (p. 42)**.

Voir Comment la police interroge et comment s'en défendre[76] pour une vue d'ensemble complète des techniques d'interrogatoire de la police.

[75] https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques
[76] https://notrace.how/resources/fr/#police-interroge

Mesures d'atténuation

Tenue anonyme (#4) : Tu peux porter une tenue anonyme dans une manifestation ou autre évènement pour que ce soit plus difficile pour une opération de surveillance visible de t'identifier.

Opérations répressives

Mauvaises intentions (#5) : Pendant une manifestation, les enquêteurs ont pris 180 photos, à partir desquelles ils ont obtenu 200 portaits des manifestant·e·s, dont dix personnes qu'ils ont pu identifier.[72]

3.22. Systèmes d'alarme

Utilisée par la tactique : **Arrestation**

Les systèmes d'alarme sont des mécanismes qui protègent les infrastructures physiques ou numériques en envoyant un signal d'alerte quand un accès non autorisé à l'infrastructure est détecté. Le signal d'alerte peut mener à l'intervention rapide d'agents de sécurité ou de la police pour investiguer la situation.

Dans le cas des infrastructures physiques, les systèmes d'alarme modernes comportent typiquement des capteurs qui détectent l'accès non autorisé à une zone en dehors des horaires de fonctionnement habituels. Ces capteurs peuvent être des détecteurs de mouvement à infrarouge, des capteurs qui détectent l'ouverture des portes, et de nombreux autres types de capteurs.[73] Le signal d'alerte peut être transmis par une connexion filiaire ou sans fil—les systèmes modernes bon marché envoient souvent le signal sur le réseau téléphonique.

Dans le cas des infrastructures numériques, les systèmes de détection d'intrusion[74] tentent de détecter toute activité qui puisse indiquer qu'un piratage est en cours. Si un accès non autorisé est détecté, une équipe d'intervention dédiée peut être alertée dans le but de contenir et de remédier à tout compromis.

[72] https://infokiosques.net/spip.php?article597
[73] https://en.wikipedia.org/wiki/Security_alarm#Sensor_types
[74] https://en.wikipedia.org/wiki/Intrusion_detection_system

Stockage

Après avoir été collectées, les images de vidéosurveillance sont souvent stockées pendant un certain temps (de quelques jours à des durées indéfinies) avant d'être effacées.

Analyse

Un adversaire peut analyser des images de vidéosurveillance :

- En temps réel si les caméras sont intégrées à un réseau centralisé. L'analyse en temps réel peut avoir lieu soit dans le cadre d'une surveillance de routine soit pour des évènements spéciaux (comme des manifestations).
- Rétroactivement si les images de vidéosurveillance ont été stockées. L'analyse rétroactive peut aider à identifier un suspect grâce à son **visage (#2)**, sa **démarche (#2)**, sa **voix (#2)**, etc.

L'analyse d'images de vidéosurveillance peut être faite :

- Par des humains.
- Par des systèmes automatisés comme les systèmes de lecture automatisée de plaques d'immatriculation ou les **systèmes de reconnaissance faciale (#2)**.

Voir aussi

- Pas vue pas prise : contre la vidéo-surveillance.[13]
- Les sujets « Vidéosurveillance »[14] et « Lecteurs de plaques d'immatriculation automatisés ».[15]

Mesures d'atténuation

Achats anonymes (#4) : Tu peux faire des achats anonymes pour empêcher un adversaire de t'identifier sur les images de vidéosurveillance de magasins physiques.

[13] https://notrace.how/resources/fr/#pas-vue
[14] https://notrace.how/resources/fr/#topic=video-surveillance
[15] https://notrace.how/resources/fr/#topic=automated-license-plate-readers

Attaque (#4) : Tu peux mettre hors d'usage[16] des caméras de surveillance.

Conversations en extérieur et sans appareils (#4) : Tu peux avoir des conversations sensibles loin de caméras de surveillance pour empêcher un adversaire d'enregistrer ces conversations avec des caméras de surveillance équipées de microphones.

Dissimulation biométrique (#4) : Si tu es filmé·e par des caméras de surveillance, tu peux :

- Pour contrer la **reconnaissance de démarche (#2)**, porter des vêtements amples qui cachent la forme de ton corps, utiliser un parapluie ou d'autres objets couvrants, ou changer drastiquement ton style de marche en adoptant une « démarche bizarre ».
- Pour contrer la **reconnaissance faciale (#2)**, porter un masque qui cache les caractéristiques de ton visage, et des lunettes de soleil ou un chapeau à bord bas pour couvrir tes yeux.

Déplacement en vélo (#4) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : comparé aux autres véhicules, un vélo est beaucoup plus difficile à identifier sur des images de vidéosurveillance, surtout si ses caractéristiques particulières sont minimisées. Par exemple, tu peux utiliser un vélo volé différent pour chaque action que tu fais.

Reconnaissance (#4) : Avant une action, tu peux identifier les positions des caméras de surveillance sur le lieu de l'action et prévoir de les éviter si possible.

Tenue anonyme (#4) : Tu peux porter une tenue anonyme pour empêcher un adversaire de t'identifier sur des images de vidéosurveillance.

Opérations répressives

Opération contre Boris (#5) : Peu après le sabotage d'avril, les enquêteurs ont récupéré les images de vidéosurveillance de commerces et de caméras municipales, et les listes de véhicules filmés par des systèmes de lecture automatisée de plaques d'immatriculation (LAPI) et des radars automatiques, tout ça dans un périmètre étendu autour du lieu du sabotage.[1]

[16] https://notrace.how/resources/fr/#detruisons-les-cameras

Opération contre Direct Action (#5) : Pendant plusieurs semaines, les enquêteurs ont suivi des membres de Direct Action et certain·e·s de leurs ami·e·s lorsqu'iels se déplaçaient à pied et en véhicules.[9]

Au moins une fois, les enquêteurs ont observé un membre de Direct Action faire des manoeuvres d'**anti-surveillance (#4)**, ce qu'ils ont trouvé suspect.

Affaire du 8 décembre (#5) : Pendant plusieurs semaines, les enquêteurs ont placé sous surveillance statique les lieux de vie de certain·e·s des inculpé·e·s et les ont suivi·e·s lorsqu'iels se déplaçaient.[43] Notamment :

- Quand les enquêteurs surveillaient le lieu de vie d'un·e inculpé·e, ils prenaient en photo toutes les personnes qui entraient ou sortaient du lieu. Si l'inculpé·e partait, iel était suivi soit par les opérateurs de surveillance surveillant le lieu de vie, soit par d'autres opérateurs pour permettre à la surveillance statique de continuer. Si l'inculpé·e partait en véhicule, iel était suivi·e en véhicule.
- Dans un cas, un·e inculpé·e a été suivi·e dans un magasin, et l'opérateur de surveillance a noté ce qu'iel achetait et l'a pris·e en photo dans le magasin.

3.21.3. Visible

La surveillance physique visible est l'observation directe de personnes ou d'activités quand les opérateurs de surveillance ont l'intention d'être détectés par leurs cibles, ou que ça ne les dérange pas d'être détectés par leurs cibles. Il s'agit d'une pratique courante lors de manifestations et rassemblements pour identifier les participants, que ce soit pour faire de la **cartographie de réseau (#1)** ou pour incriminer des personnes pour des actions réalisées pendant la manifestation.

La surveillance physique visible de seulement quelques individus est rare, et a plus souvent pour objectif de créer de la paranoïa pour dissuader que d'incriminer.

l'incendie ont indiqué qu'ils pensaient que le feu était d'origine volontaire, les incendiaires ont été arrêtés.

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs :[3]

- Ont suivi l'une des personnes arrêtées pendant quelques heures une fois, et pendant quelques minutes une autre fois, pour découvrir où elle habitait.
- Ont passé plusieurs jours à faire une surveillance statique d'un lieu associé à la lutte contre Cigéo (quelques bâtiments isolés entourés par des champs). Pendant jusqu'à 16 heures par jour ils ont noté et photographié les personnes et véhicules rejoignant et quittant le lieu.

Les trois du banc public (#5) : Au cours de la soirée précédant l'arrestation, deux des personnes ont roulé en vélo à travers la ville et ont été suivies par des policiers en vélo (et probablement aussi des policiers en voiture) jusqu'à leur arrestation dans le parc.[25] Les policiers ont décidé de suivre les personnes ce soir là en particulier car cela faisait exactement deux ans depuis le sommet du G20 à Hambourg et qu'elles étaient suspectées de prévoir une action pour l'anniversaire du sommet.

Operation 8 (#5) : Les enquêteurs ont régulièrement suivi des personnes à pied et en véhicule.[69]

Les enquêteurs ont régulièrement mené des opérations de surveillance cachée près des « camps d'entraînement », mais n'ont pas pu s'approcher suffisamment pour voir ce qui s'y passait et n'ont pu qu'entendre des coups de feu.[3]

Opération à Nea Filadelphia (#5) : Le jour des arrestations, quand une personne a visité un cybercafé qui était probablement sous surveillance policière, des policiers l'ont reconnue et se sont mis à la suivre.[70] Elle s'est ensuite déplacée à travers les rues d'Athènes pendant quelques heures, rejoignant petit à petit les autres personnes—dont certaines étaient recherchées par la police[71]—et tout le monde a été arrêté.

[69] https://putatara.net/2013/11/25/operation-8-the-evidence

[70] https://web.archive.org/web/20201027031238/http://actforfree.nostate.net/?p=15472

[71] https://machorka.espivblogs.net/2013/11/06/letter-from-anarchists-argiris-dalios-and-fivos-harisis-from-koridallos-prisons-athens

Opération de 2019-2020 contre Mónica et Francisco (#5) : Des images de vidéosurveillance publique ont été amplement utilisées par les enquêteurs pour reconstruire les déplacements de Mónica et Francisco avant et durant les actions, malgré les mesures d'atténuation qu'iels ont prises (prendre des taxis, changer de vêtements, porter des déguisements).[5]

Répression contre Zündlumpen (#5) : Trois mois avant un incendie volontaire, une caméra de surveillance de la faune sauvage a filmé une personne qui portait une veste orange en train de marcher.[17] Après l'incendie, les enquêteurs ont obtenu les images de la caméra et ont affirmé que la veste ressemblait à une veste portée à un moment par M.

Opération contre Revolutionära fronten (#5) : Les images de vidéosurveillance de caméras situées près du lieu du tabassage de Stockholm ont montré que certain·e·s des inculpé·e·s étaient présent·e·s lors du tabassage.[3]

Répression du sabotage de l'usine Lafarge (#5) : Immédiatement après l'action, les enquêteurs ont obtenu les images de vidéosurveillance de transports en commun (bus, gares, etc.), de commerces, de caméras de surveillance de maisons privées et de caméras municipales, le tout dans un périmètre étendu autour du lieu de l'action.[18] Les images de l'intérieur des bus semblent notamment avoir aidé à identifier des personnes qui s'étaient déplacées vers et depuis le lieu de l'action.[19] Les enquêteurs ont aussi obtenu les images de péages d'autoroute, vraisemblablement pour identifier les personnes à l'intérieur de voitures suspectées d'avoir emprunté l'autoroute vers ou depuis le lieu de l'action.

Prometeo (#5) : Deux des personnes ont prétendumment été vues sur des images de vidéosurveillance quitter un magasin où les enquêteurs pensent que les enveloppes utilisées pour préparer les colis piégés ont été achetées.[20]

Arrestation de Stecco (#5) : Les enquêteurs ont analysé les images de vidéosurveillance de caméras de rues, de gares, de péages d'autoroute, de

[17] https://de.indymedia.org/node/548259

[18] https://notrace.how/resources/fr/#lafarge

[19] https://sansnom.noblogs.org/archives/16831

[20] https://ilrovescio.info/2020/08/23/uno-scritto-di-natascia-dal-carcere-di-piacenza

bus et de commerces afin de déterminer les déplacements de personnes sous surveillance.[6]

Opération de 2013 contre Mónica et Francisco (#5) : Des images de vidéosurveillance publique ont été utilisées pour reconstruire les déplacements de Mónica et Francisco avant et après l'action.[21] Cela a montré qu'iels étaient près du lieu de l'action peu avant l'explosion de l'engin.

Opération contre Peppy et Krystal (#5) : Des images de vidéosurveillance d'un bus ont permis aux enquêteurs d'identifier la plaque d'immatriculation de la moto sur laquelle Peppy et Krystal sont arrivés au lieu de la manifestation et en sont partis.[22]

Opération contre Louna (#5) : Les images de vidéosurveillance du lieu de l'incendie ont montré deux personnes mettre le feu à la pelleteuse, et l'une d'entre elles être victime d'un retour de flamme.[23]

Les images de vidéosurveillance de l'hôpital la nuit de l'incendie ont montré :

- La plaque d'immatriculation de la voiture qui a amené Louna à l'hôpital.
- Les visages des autres personnes de la voiture.
- L'une des personnes de la voiture transportant un arrosoir. Les enquêteurs tenteront plus tard de trouver cet arrosoir dans une perquisition.

Les images de vidéosurveillance de caméras de plusieurs municipalités ont été utilisées pour essayer de reconstruire le trajet de la voiture qui a amené Louna à l'hôpital, et le trajet de Louna quand elle a quitté l'hôpital.[3]

Répression du premier incendie de Jane's Revenge (#5) : Des images de vidéosurveillance ont aidé à identifier un véhicule conduit par la personne, lorsqu'elle a été vue entrer dans un parking à pied après une manifestation, et que le véhicule a été vu quitter ce même parking quelques minutes

[21] https://notrace.how/documentation/monica-and-francisco-2013-case-file.pdf

[22] https://notrace.how/documentation/case-against-peppy-and-krystal-affidavit.pdf

[23] https://soutienlouna.noblogs.org/post/2025/01/23/free-louna-des-nouvelles-de-laffaire-de-louna-meuf-trans-anar-incarceree-dans-le-cadre-de-la-lutte-contre-la69

- Le 8 octobre, ils ont :
  - De nouveau surveillé pendant 6 heures les domiciles des parents et des grand-parents de Louna.
  - Effectué plusieurs passages en véhicule devant les domiciles de plusieurs membres de la famille de Louna, et d'une personne l'ayant accompagné à l'hôpital.
  - De nouveau suivi pendant 6 heures une personne qui avait été vue avec Louna à l'hôpital.
- Le 10 octobre, lors du procès d'une personne opposée au projet d'autoroute, ils ont surveillé l'intérieur et les abords du tribunal.
- Le 12 octobre, après avoir entendu parlé d'un rendez-vous devant des immeubles résidentiels via une écoute téléphonique, ils ont surveillé ces immeubles et arrêté deux personnes s'étant rendues au rendez-vous, dont Louna.

Répression du premier incendie de Jane's Revenge (#5) : En mars 2020, des policiers ont observé secrètement la personne à une distance d'environ 30 mètres.[24] Les policiers ont regardé la personne jeter un sac, l'ont récupéré, et ont prélevé des preuves ADN reliant la personne au lieu de l'action.

Opération contre Jeff Luers (#5) : La nuit de l'incendie de juin, les incendiaires étaient suivis par une équipe de surveillance—des policiers dans une ou plusieurs voitures en civil—alors qu'ils conduisaient vers le lieu de l'incendie.[68] Ils ont garé leur voiture proche du lieu de l'incendie, sous l'oeil de l'équipe de surveillance. Ils sont sortis de leur voiture pour continuer à pied, et l'équipe de surveillance les a perdus de vue. Ils sont revenus en courant vers leur voiture 10 minutes plus tard, et l'équipe de surveillance s'est remise à les observer. Ils ont quitté en voiture le lieu de l'incendie. Plus d'une heure plus tard, l'équipe de surveillance—qui suivait toujours les incendiaires—a entendu parler, sur le système de communication radio de la police, d'un feu sur le lieu de l'incendie et a demandé à des policiers locaux d'arrêter la voiture des incendiaires pour un contrôle routier, suspectant qu'ils avaient quelque chose à voir avec le feu. Une demi-heure plus tard, quand les experts incendie sur le lieu de

[68] https://courtlistener.com/opinion/2627996/state-v-luers

Quelques jours après la manifestation, les enquêteurs ont mis en place une surveillance physique discrète du domicile de Peppy et Krystal. Ils ont observé Peppy et Krystal conduire la même moto qu'iels avaient utilisée pour arriver au lieu de la manifestation et en partir.

Opération de 2011-2013 contre Jeremy Hammond (#5) : Pendant une opération de surveillance physique contre le domicile de Jeremy Hammond ayant duré plusieurs jours, les enquêteurs ont établi une corrélation entre :[2]

- Les moments où Jeremy Hammond était présent physiquement chez lui.
- Et les moments où son identité numérique était signalée comme étant en ligne par l'informateur Sabu.

Opération contre Louna (#5) : Suite à l'incendie dans la nuit du 4 au 5 mai 2024, les enquêteurs ont mené plusieurs opérations de surveillance physique :[3]

- Le 5 mai, à l'hôpital, ils ont pris en photo des personnes demandant des nouvelles de Louna et écouté des conversations.
- Les 6, 7, 11 et 14 mai, ils ont surveillé deux lieux où habitaient des personnes opposées au projet d'autoroute. Ils ont pris des photos et relevé des plaques d'immatriculation de véhicules.
- Le 10 mai, ils ont surveillé l'entrée de l'hôpital, où Louna avait un rendez-vous.
- En juillet, ils ont surveillé un évènement organisé par une personne opposée au projet d'autoroute.

Début octobre, Louna a fait l'objet d'un mandat de recherche. Jusqu'à son arrestation le 12 octobre 2024, les enquêteurs ont mené plusieurs opérations de surveillance physique :

- Le 3 octobre, ils ont :
  - Surveillé pendant 6 heures les domiciles des parents et des grand-parents de Louna.
  - Effectué plusieurs passages en véhicule devant un autre domicile de la famille de Louna.
  - Suivi pendant 4 heures une personne qui avait été vue avec Louna à l'hôpital.

plus tard.[24]

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont utilisé des images des manifestations, filmées par des caméras de surveillance ou des policiers, pour :[3]

- Identifier une personne qui n'était que partiellement masquée, avec ses yeux, ses lunettes et son front visibles.
- Faire le lien entre une personne qui avait l'air enceinte au vu de son ventre, vue dans une manifestation, et une personne qui a accouché quelques mois plus tard.

Les trois du banc public (#5) : Dans la soirée précédant l'arrestation, une des personnes—alors qu'elle était suivie par des policiers—s'est arrêtée à une station-service et a été vue par les caméras de vidéosurveillance de la station acheter de l'essence et remplir un bidon d'essence.[25] Les policiers ont obtenu les images de vidéosurveillance le matin suivant.

Opération contre Ruslan Siddiqi (#5) : Des images de vidéo-surveillance d'usines près du site de l'attaque à l'explosif contre le train ont montré une personne se déplaçant à vélo peu avant et après l'attaque, portant une veste de camouflage et un sac à dos.[8] Cela a contribué à la théorie que la personne ayant mené l'attaque s'était déplacée à vélo.

Répression de l'attaque sur le siège de Clarín (#5) : Les images de vidéosurveillance provenant de plusieurs caméras ont montré l'un·e des inculpé·e·s quitter le lieu de l'attaque, se faire conduire en moto sur quelques rues, puis monter dans un bus—l'inculpé·e a été identifié·e car iel a utilisé la carte électronique de bus de son/sa partenaire pour monter dans le bus.[26]

[24] https://notrace.how/documentation/first-jane-s-revenge-arson-investigation-files.pdf

[25] https://notrace.how/resources/fr/#parkbank

[26] https://web.archive.org/web/20211210123411/https://www.revolucionpopular.com/otras-noticias/la-policia-detuvo-a-otro-hombre-por-el-ataque-a-clarin_a61b34174d2f0a04884749d24

3.20. Surveillance numérique ciblée

Utilisée par la tactique : **Incrimination**

La surveillance numérique ciblée est la collecte et l'analyse ciblées de données et communications numériques.

Des techniques extrêmement avancées existent[27] dans l'arsenal des acteurs étatiques, mais on va se concentrer ici sur les techniques qui ont plus de chances d'être utilisées contre des anarchistes et autres rebelles.

Voir le sujet « Surveillance numérique ».[11]

3.20.1. Accès physique

L'accès physique est le processus par lequel un adversaire accède physiquement à un appareil électronique afin d'accéder à ses données ou de le compromettre.

Voici des exemples notables d'appareils électroniques auxquels un adversaire peut accéder physiquement :

- Des ordinateurs, téléphones, et supports de stockage (par exemple des disques dur, clés USB, cartes SD).
- Des imprimantes, appareils photos, télévisions « intelligentes ».
- Des véhicules. Par exemple, les systèmes embarqués[28] des véhicules modernes peuvent stocker l'historique des positions du véhicule.

Si un adversaire accède physiquement à un appareil, il peut :

- Lire les données non chiffrées de l'appareil, ou ses données chiffrées si il est allumé (et donc que son **chiffrement (#4)** n'est pas efficace).
- Compromettre l'appareil avec un **malware (p. 22)**.
- Compromettre l'appareil avec un enregistreur de frappes matériel.[29]

Un adversaire peut accéder physiquement à un appareil :

[27] https://anonymousplanet.org/guide/some-advanced-targeted-techniques
[28] https://fr.wikipedia.org/wiki/Système_embarqué_mobile
[29] https://en.wikipedia.org/wiki/Hardware_keylogger

Trois jours auparavant, les enquêteurs avaient obtenu l'adresse du domicile grâce à la collaboration du Supplemental Nutrition Assistance Program,[67] et avaient également obtenu la liste des achats effectués via le programme dans les trois mois précédents. L'opérateur a vu quelqu'un qui correspondait à la description de la personne quitter le domicile en voiture, mais n'a pas pu le/la suivre parce qu'iel « allait trop vite ». L'opérateur s'est alors rendu à la boutique d'une station-service voisine qui figurait fréquemment sur la liste d'achats. L'opérateur y a retrouvé la personne. L'opérateur a demandé à un·e policier qui se trouvait là de l'aider à arrêter la personne, mais le/la policier a refusé, en partie parce qu'iel n'était pas là « en sa capacité d'agent de maintien de l'ordre ». L'opérateur a alors demandé l'aide de la police d'État, mais avant que celle-ci ne puisse intervenir, la personne était repartie de la station-service. Alors que la personne s'éloignait en voiture, l'opérateur a tenté de saisir son poignet. Quinze minutes plus tard, l'opérateur est passé en véhicule devant le domicile et a vu la personne partir dans le siège passager d'un véhicule, mais n'a pas pu la suivre à cause d'une circulation trop dense.

Arrestation de Stecco (#5) : Les enquêteurs ont appris grâce à un micro caché installé dans un domicile qu'une personne sous surveillance allait voyager en train le lendemain.[6] Le lendemain, cette personne et une autre ont effectivement voyagé en train et un grand nombre d'opérateurs de surveillance ont été déployés pour les suivre. Il y avait quatre opérateurs dans le train (deux à chaque extrémité) et deux opérateurs qui attendaient à chaque gare intermédiaire.

Opération contre Peppy et Krystal (#5) : Une semaine avant la manifestation, les enquêteurs ont mis en place une surveillance physique discrète d'une bibliothèque locale où ils savaient que des personnes qui planifiaient la manifestation s'organisaient.[22] Ils ont observé Peppy entrer dans la bibliothèque et en partir une heure et demie plus tard.

[67] Le Supplemental Nutrition Assistance Program (SNAP, *Programme d'aide supplémentaire à la nutrition*) est un programme gouvernemental d'aide à l'achat de denrées alimentaires. Chaque mois, les bénéficiaires reçoivent de l'argent sur une carte de débit spéciale qui fait partie d'un système électronique appelé « electronic benefit transfer » (EBT, *transfert électronique de prestations*). Les bénéficiaires peuvent utiliser la carte pour acheter de la nourriture.

suffisamment d'informations sur les activités de la cible pour l'incriminer et juge nécessaire d'arrêter la cible immédiatement (par exemple pour l'empêcher de commettre un crime).

Voir aussi

- Surveillance Countermeasures[64] (*Mesures contre la surveillance*) à propos des principes et techniques de la surveillance physique cachée.
- Maßnahmen gegen Observation[65] (*Mesures contre la surveillance*) pour un aperçu de comment les agences de police et de renseignement pratiquent la surveillance physique cachée.
- Le sujet « Surveillance physique ».[66]

Mesures d'atténuation

Anti-surveillance (#4) : Tu peux faire de l'anti-surveillance pour échapper à une opération de surveillance physique cachée.

Déplacement en vélo (#4) : Tu peux utiliser un vélo plutôt qu'un autre type de véhicule : comparé aux autres véhicules ou à des personnes à pied, un vélo est plus difficile à suivre par une opération de surveillance physique cachée, surtout sans que l'opération soit détectée.

Détection de surveillance (#4) : Tu peux faire de la détection de surveillance pour détecter une opération de surveillance physique cachée.

Opérations répressives

Opération contre Boris (#5) : Pendant plusieurs semaines, les enquêteurs ont régulièrement surveillé le domicile de Boris et l'ont suivi lorsqu'il se déplaçait à pied, à vélo, et dans des véhicules.[1]

Répression contre Zündlumpen (#5) : Les enquêteurs ont suivi N. pendant 15 jours.[42]

Recherche d'un·e fugitive (#5) : En 2022, un opérateur de surveillance a mené, seul, une opération de surveillance physique cachée d'un domicile.[3]

[64] https://notrace.how/resources/fr/#surveillance-countermeasures
[65] https://notrace.how/resources/fr/#gegen-observation
[66] https://notrace.how/resources/fr/#topic=physical-surveillance

- Pendant une **perquisition (#1)** ou une **visite discrète de domicile (p. 45)**.
- Après t'avoir arrêté si tu as l'appareil sur toi.
- Pendant un contrôle aux frontières.
- Via un·e **infiltré·e (#1)** ou un·e **indic (#1)** qui a accès à l'appareil.

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#4) : Tu peux faire une analyse des ordinateurs et téléphones pour détecter si un appareil a été accédé physiquement par un adversaire.

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques pour contrer le risque qu'un adversaire accède physiquement à tes appareils numériques. Par exemple, si tu vas à un évènement ou une manifestation et que tu penses que tu pourrais être arrêté·e, tu ne devrais pas prendre ton téléphone avec toi.

Dessiner une carte de son réseau (#4) : Un adversaire pourrait accéder physiquement à tes appareils numériques via un·e **infiltré·e (#1)** ou un·e **indic (#1)**. Pour contrer ça, tu peux dessiner une carte de ton réseau pour t'aider à identifier les personnes en qui tu fais assez confiance pour les laisser accéder à tes appareils numériques.

Détection d'intrusion physique (#4) : Tu peux prendre des mesures de détection d'intrusion physique pour détecter quand un espace a été accédé physiquement par un adversaire.

Mesures de détection d'accès physique (#4) : Tu peux prendre des mesures de détection d'accès physique pour détecter quand quelque chose a été accédé physiquement par un adversaire.

3.20.2. Contournement de l'authentification

Le contournement de l'authentification est le processus par lequel un adversaire contourne le **chiffrement complet du disque (#4)** qui protège l'accès à un appareil numérique. Un adversaire peut contourner l'authentification grâce à des erreurs humaines, des mots de passe faibles, ou des failles techniques.

Un adversaire peut contourner l'authentification des manières suivantes :

- Accéder à un appareil alors qu'il est allumé (et donc que son chiffrement n'est pas efficace).
- Trouver le mot de passe de chiffrement écrit quelque part.
- Forcer le propriétaire de l'appareil à fournir le mot de passe de chiffrement en utilisant des **techniques d'interrogatoire (p. 38)**, y compris, dans certains contextes, de la **violence physique (p. 42)**.
- Interception visuelle : observer le propriétaire de l'appareil taper le mot de passe de chiffrement via une **caméra cachée (#1)** ou un·e **infiltré·e (#1)** ou **indic (#1)**.
- Brute force : deviner le mot de passe de chiffrement via des tentatives d'authentification automatiques et répétées.
- Compromettre l'appareil numérique avec un **malware (p. 22)** installé à distance ou en **accédant physiquement (p. 15)** à l'appareil.
- Exploiter une faille au niveau de l'implémentation du processus de chiffrement.

Mesures d'atténuation

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser des systèmes d'exploitation axés sur la sécurité avec un chiffrement complet du disque et des mots de passe robustes, pour que ce soit plus difficile pour un adversaire de contourner l'authentification de tes appareils numériques. Par exemple :

- Sur des ordinateurs, tu peux utiliser le chiffrement complet du disque de Linux appelé LUKS, qui est utlisé par de nombreux systèmes Linux, dont Debian[30] et Tails,[31] et que le service de police scientifique de la police fédérale allemande n'a pas pu déchiffrer après avoir essayé pendant une année.[32]
- Sur des téléphones, tu peux utiliser GrapheneOS, dont le chiffrement complet du disque fait qu'il est plus difficile pour un adversaire de

[30] https://debian.org
[31] https://tails.net/index.fr.html
[32] https://notrace.how/resources/fr/#parkbank

l'équipe de surveillance doit utiliser des véhicules, mais si la cible est à pied, l'équipe de surveillance peut préférer utiliser des opérateurs à pied.
- Se mettre à couvert et se dissimuler pour éviter d'être détecté par la cible. Par exemple, des véhicules de surveillance peuvent se cacher derrière d'autres véhicules, et des opérateurs de surveillance à pied peuvent se cacher parmi les autres piétons.
- Faire tourner l'opérateur ou le véhicule de surveillance le plus proche de la cible pour limiter le risque que la cible remarque qu'elle est suivie.

La surveillance physique mobile peut être facilitée par :

- Un **dispositif de surveillance par localisation (#1)** installé sur le véhicule ou le vélo de la cible.
- La géolocalisation en temps réel du téléphone de la cible, obtenue grâce à la **collaboration des opérateurs de téléphonie mobile (#1)**.
- Une **surveillance aérienne (p. 27)**, par exemple un drone qui suit la cible de loin.

Statique

La surveillance physique statique est l'observation d'une cible quand la cible ne peut pas bouger, ou que les opérateurs de surveillance n'ont pas l'intention de la suivre si elle bouge. Une opération de surveillance physique statique est typiquement menée par une équipe de surveillance utilisant un ou plusieurs véhicules.

Un exemple d'une opération de surveillance physique statique est de garer un véhicule de surveillance devant le domicile d'une cible, avec des opérateurs de surveillance à l'intérieur du véhicule observant l'entrée du domicile.

Arrestation

Généralement, une équipe de surveillance ne va pas tenter d'arrêter sa cible au cours d'une opération de surveillance physique cachée. Dans de rares cas, cependant, cela peut se produire si l'équipe de surveillance a obtenu

Operation 8 (#5) : Le matin des perquisitions du 15 octobre un hélicoptère de la police survolait une zone où plusieurs perquisitions avaient lieu, apparemment pour surveiller les lieux.[62]

Répression du soulèvement de 2019 au Chili (#5) : Des drones ont été utilisés pour suivre les émeutièr·e·s qui quittaient les émeutes pour pouvoir les arrêter.[63]

Opération contre Direct Action (#5) : Après que les enquêteurs aient découvert la zone isolée où les membres de Direct Action cachaient les explosifs volés qu'iels utilisaient dans les attaques à l'explosif, ils ont pris des dispositions pour qu'un hélicoptère survole la zone chaque jour pour la surveiller.[9]

3.21.2. Cachée

La surveillance physique cachée est l'observation directe de personnes ou d'activités quand les opérateurs de surveillance ne veulent pas être détectés par leurs cibles.

Mobile

Une opération de surveillance physique mobile est typiquement menée par une équipe de surveillance de cinq à vingt opérateurs utilisant plusieurs véhicules, et commence typiquement par une phase statique : surveiller l'endroit où la cible est présumée se trouver, comme son domicile ou son lieu de travail. Quand la cible quitte la zone de surveillance statique, l'équipe de surveillance se met à la suivre et l'opération de surveillance transitionne vers une phase mobile. L'opération de surveillance alterne ensuite entre des phases statiques (quand la cible s'arrête) et des phases mobiles (quand la cible se remet en mouvement).

Voici des exemples de techniques de surveillance physique mobile :

- Utiliser un moyen de transport approprié en fonction du moyen de transport de la cible. Par exemple, si la cible est dans un véhicule,

[62] https://rebelpress.nz/wp-content/uploads/2021/03/Day_Raids_Came.pdf

[63] https://es-contrainfo.espiv.net/2019/11/06/chile-una-mirada-anarquica-al-contexto-de-revuelta-y-represion

deviner le mot de passe de chiffrement par brute force : après 140 essais ratés, chaque essai est retardé d'un jour complet.[33]

Mesures de détection d'accès physique (#4) : Tu peux prendre des mesures de détection d'accès physique pour détecter si un appareil a été **accédé physiquement (p. 15)**.

Une fois qu'un appareil a été accédé physiquement par un adversaire, tu devrais le considérer comme compromis et ne plus jamais t'authentifier dessus. En effet, dans le pire des cas, l'adversaire pourrait avoir copié les données de l'appareil et avoir compromis son firmware de telle sorte que quand tu entres ton mot de passe, il peut l'obtenir à distance et l'utiliser pour déchiffrer les données.

Recherche de dispositifs de surveillance (#4) : Avant d'entrer un mot de passe dans une pièce où des **dispositifs de surveillance cachés vidéo (#1)** pourraient être présents, tu peux faire une recherche de dispositifs de surveillance pour localiser de tels dispositifs et les retirer.

Opérations répressives

Répression contre Zündlumpen (#5) : Dans certaines des perquisitions, les policiers ont saisi des smartphones immédiatement après être entrés et les ont branchés à des batteries externes, vraisemblablement pour les empêcher de s'éteindre, ce qui aurait ré-activé leur chiffrement.[34]

Les arrestations de février de N. et M. ont eu lieu dans une bibliothèque publique, alors que N. et M. utilisaient un ordinateur.[35] Des agents de police en civil ont attendu que N. et M. déverrouillent l'ordinateur pour se révéler et mener l'arrestation, vraisemblablement pour accéder à l'ordinateur alors qu'il était déverrouillé.

Répression du sabotage de l'usine Lafarge (#5) : Les enquêteurs ont saisi plusieurs smartphones chiffrés dans les perquisitions et ont tenté d'accéder à leurs données chiffrées, avec plus ou moins de succès en fonction des téléphones :[18]

[33] https://grapheneos.org/faq#encryption

[34] https://sansnom.noblogs.org/archives/12094

[35] https://sansnom.noblogs.org/archives/26261

- Pour les iPhones qui ont été saisis allumés, ils ont exploité les failles de sécurité qui existent quand ils sont allumés pour contourner leur chiffrement et accéder aux données chiffrées.
- Pour tous les téléphones Android (qu'ils aient été saisis allumés ou éteints) et pour un iPhone saisi éteint, ils ont extrait les partitions chiffrées des téléphones et ont tenté de deviner leurs mots de passe par *brute force* depuis un ordinateur.

Arrestation de Stecco (#5) : Les enquêteurs ont trouvé le code PIN du smartphone d'une personne sous surveillance lorsqu'une caméra cachée dans une voiture a filmé cette personne en train de saisir le code.[6]

Les enquêteurs ont tenté de trouver le mot de passe d'un système Tails par « brute force » à l'aide d'un logiciel nommé « bruteforce-luks ».

Opération de 2011-2013 contre Jeremy Hammond (#5) : Les enquêteurs ont contourné l'authentification de l'ordinateur portable chiffré de Jeremy Hammond, qu'ils avaient saisi lors de la perquisition de mars 2012.[36] Ils ont vraisemblablement réalisé le contournement en devinant le mot de passe de l'ordinateur, qui était un mot de passe très simple—soit « chewy123 »,[37] soit « chewy12345 ».[38]

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont contourné l'authentification de cinq disques dur chiffrés trouvés dans des perquisitions :[3]

- Un disque dur grâce au mot de passe très simple « stopcigeo », qu'ils ont peut-être deviné.
- Un disque dur grâce à un mot de passe trouvé sur un post-it sous l'ordinateur contenant le disque dur.
- Un disque dur grâce à un mot de passe qui leur a été donné par le/la propriétaire de l'ordinateur contenant le disque dur.
- Deux disques durs grâce à des mots de passe qu'ils ont trouvé dans un document texte sur un disque dur préalablement déchiffré.

[36] https://apnews.com/domestic-news-domestic-news-general-news-abae6d15cbf04d75bbbc58225a470f98

[37] Selon des articles de presse.

[38] Selon *American Kingpin* (Nick Bilton, 2017).

aérienne de te suivre : un métro souterrain, un centre commercial avec beaucoup d'entrées, etc.

Attaque (#4) : Pendant une manifestation, tu peux abattre des drones avec des feux d'artifice, les pirater, ou les aveugler avec des lasers. Voir aussi Cinq manières à la portée de tous pour abattre un drone.[59]

Détection de surveillance (#4) : Tu peux faire de la détection de surveillance pour détecter la plupart des hélicoptères et certains drones en tendant l'oreille à de potentiels hélicoptères et drones : tu devrais entendre la plupart d'entre eux, selon leur altitude et l'endroit où tu te trouves.

Tenue anonyme (#4) : Si tu es suivi·e par une opération de surveillance aérienne, tu peux te changer et mettre une tenue anonyme quand tu es dans un endroit qui n'est pas visible depuis le ciel pour que ce soit plus difficile pour l'opération de surveillance aérienne de te retrouver quand tu émergeras dans un endroit visible (ça ne fonctionnera pas si l'opération de surveillance t'observe également depuis le sol).

Opérations répressives

Répression contre Zündlumpen (#5) : Des drones ont été utilisés pour suivre N. et M. dans une forêt pendant une opération de surveillance physique cachée.[17]

Conspiration sur un chemin de fer à Berlin en 2023 (#5) : Les personnes arrêtées ont été découvertes de nuit par un hélicoptère au cours d'un vol de surveillance de routine, vraisemblement muni d'équipement de vision nocture.[60] Un texte[61] relate qu'en 2022, lors d'un autre vol de surveillance de routine près de Berlin, ce même hélicoptère avait éteint ses feux de navigation et étouffé le son des pales de son rotor pour éviter d'être détecté : « Bien qu'on puisse toujours entendre l'hélicoptère, il faisait moins de bruit. Cela peut mener à sous-estimer la distance de l'hélicoptère, ou, si d'autres bruits sont présents comme une autoroute, à ne pas se rendre compte du problème en approche avant qu'il ne soit trop tard. »

[59] https://notrace.how/resources/fr/#cinq-manieres

[60] https://notrace.how/resources/fr/#on-conspire

[61] https://kontrapolis.info/9821

3.21.1. Aérienne

La surveillance physique aérienne est l'observation directe de personnes ou d'activités dans le but d'obtenir des informations. Dans de nombreux pays, les hélicoptères ont traditionnellement été le principal outil pour ce type de surveillance. Les drones devenant moins coûteux, leur utilisation devient plus courante. Les avions de surveillance sont aussi utilisés occasionnellement et sont bien plus discrets que les hélicoptères.

Voici des exemples de surveillance physique aérienne :

- Observer la foule pendant des manifestations ou rassemblements, souvent dans le cadre d'une opération de surveillance **visible (p. 36)**.
- Améliorer les chances de suivre la cible de la surveillance avec succès lors d'une opération de surveillance **cachée (p. 29)**, notamment de nuit.
- Localiser des suspects peu après qu'une action ait eu lieu et que l'adversaire ait été alerté, notamment dans des zones rurales ou de nuit (dans le cas d'un incendie volontaire en Allemagne, un hélicoptère de la police est intervenu en volant au-dessus de la zone la nuit de l'incendie[55]).
- Localiser des suspects dans le cadre de **patrouilles de police (#1)** de routine dans des zones où le risque d'activité criminelle est élevé.

Les avions de surveillance peuvent surveiller des villes entières, photographiant jusqu'à 80 kilomètres carrés par seconde, permettant de reconstruire au ralenti presque tout mouvement en extérieur,[56] avec des images de haute qualité de nuit.[57]

Voir le sujet « Surveillance aérienne ».[58]

Mesures d'atténuation

Anti-surveillance (#4) : Tu peux inclure dans un itinéraire d'anti-surveillance des endroits qui empêcheraient une opération de surveillance

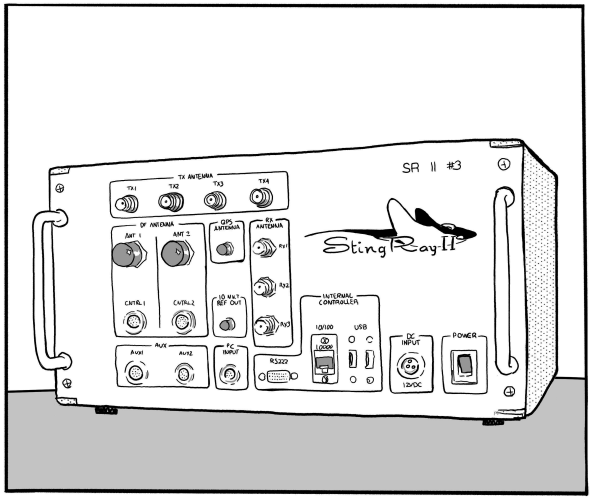
[55]https://actforfree.noblogs.org/post/2023/11/13/munich-germany-geothermal-energy-gets-hot-and-not-only

[56]https://theintercept.com/2020/04/09/baltimore-police-aerial-surveillance

[57]https://theintercept.com/document/2021/08/31/motion-to-suppress-aerial-surveillance-evidence-in-u-s-vs-muhammed-momtaz-alazhari

[58]https://notrace.how/resources/fr/#topic=aerial-surveillance

3.20.3. IMSI-catcher



Un IMSI-catcher (aussi connu sous le nom de *Stingray*) est un appareil utilisé pour collecter des informations à propos de tous les téléphones allumés dans une zone restreinte (de quelques mètres à plusieurs centaines de mètres) autour de lui. Un IMSI-catcher passif écoute simplement le traffic, alors qu'un IMSI-catcher actif agit comme une « fausse » antenne téléphonique entre les téléphones et les vraies antennes téléphoniques.

Un IMSI-catcher peut collecter les informations suivantes à propos des téléphones autour de lui :

- Leurs numéros.
- Leurs numéros IMSI[39] et IMEI.[40]
- Des données et métadonnées à propos de leur activité : le contenu des SMS et appels classiques, la liste des sites web visités, des métadonnées à propos de leur utilisation d'applications de messagerie chiffrées de bout-en-bout (par exemple, quand est-ce que Signal est utilisé et la taille approximative des messages envoyés ou reçus sur Signal).

[39]Un numéro International Mobile Subscriber Identity (IMSI, *identité internationale d'abonné mobile*) est un numéro qui identifie une carte SIM de manière unique.

[40]Un numéro International Mobile Equipment Identity (IMEI, *identité internationale d'équipement mobile*) est un numéro qui identifie un téléphone de manière unique.

Un adversaire peut utiliser un IMSI-catcher pour relier des personnes et des numéros de téléphone. Par exemple :

- Pendant une manifestation, pour enregistrer les numéros de téléphone de tous les téléphones présents à la manifestation et ensuite obtenir les noms associés à ces numéros de téléphone grâce à la **collaboration des opérateurs de téléphonie mobile (#1)**.
- Dans le cadre d'une opération de **surveillance physique (p. 26)** pour trouver le numéro de téléphone de la cible ou les numéros de téléphone des personnes en contact avec la cible.

Un adversaire peut aussi utiliser un IMSI-catcher pour enregistrer l'activité d'un téléphone. Par exemple :

- Pour enregistrer l'activité d'un téléphone cible sans avoir besoin de la collaboration de l'opérateur de téléphonie mobile (qui, dans certains contextes, peut nécessiter un mandat).
- Pour enregistrer l'activité d'un téléphone cible quand l'adversaire sait où le téléphone est utilisé, mais ne connaît pas son numéro.

Voir le sujet « IMSI-catchers ».[41]

Mesures d'atténuation

Chiffrement (#4) : Tu peux chiffrer les données « en mouvement » d'un téléphone pour que si les données sont collectées par un IMSI-catcher, elles ne puissent pas être analysées. Par exemple, tu peux utiliser des applications de messagerie chiffrées de bout-en-bout plutôt que des SMS et appels classiques pour tes communications téléphoniques.

Recherche de dispositifs de surveillance (#4) : Tu peux faire une recherche de dispositifs de surveillance pour détecter la présence d'un IMSI-catcher.

Détecter la présence d'un IMSI-catcher peut avoir plusieurs avantages :

- La présence d'un IMSI-catcher est un bon indice du niveau de surveillance mis en place par un adversaire.
- Si l'IMSI-catcher est utilisé dans un évènement ou une manifestation, sa présence peut t'aider à convaincre les participant·e·s d'éteindre leurs téléphones.

[41] https://notrace.how/resources/fr/#topic=imsi-catchers

Chiffrement (#4) : Tu peux chiffrer des données « en mouvement » pour que ce soit plus difficile pour un adversaire d'analyser ces données grâce à la science forensique appliquée aux réseaux informatiques.

Cloisonnement (#4) : Un adversaire peut établir des liens entre différentes identités numériques grâce aux empreintes laissées par leurs traffics réseau. Pour contrer ça, tu peux cloisonner différentes identités numériques en :

- Utilisant Tails[31] et en redémarrant entre chaque session.
- Utilisant Qubes OS[51] avec différentes machines virtuelles Whonix[54] que tu n'utilises pas simultanément.

Opérations répressives

Opération de 2011-2013 contre Jeremy Hammond (#5) : Pendant plusieurs jours, les enquêteurs ont analysé le traffic réseau du routeur utilisé par Jeremy Hammond pour établir une corrélation entre :[2]

- Les moments où le traffic indiquait l'utilisation du réseau Tor.
- Et les moments où l'identité numérique de Jeremy Hammond était signalée comme étant en ligne par l'informateur Sabu.

3.21. Surveillance physique

Utilisée par la tactique : **Incrimination**

La surveillance physique est l'observation directe de personnes ou d'activités dans le but d'obtenir des informations. Une *opération de surveillance physique* est typiquement menée par une ou plusieurs *équipes de surveillance* composées d'individus ayant reçu une formation spécifique appelés des *opérateurs de surveillance*.

Parce qu'elle nécessite le déploiement d'opérateurs de surveillance sur le terrain, parfois pour de longues périodes, la surveillance physique est une méthode de surveillance coûteuse en ressources et en personnel.

[54] https://whonix.org

3.20.5. Science forensique appliquée aux réseaux informatiques

La science forensique appliquée aux réseaux informatiques est la surveillance et l'analyse de traffic réseau.

Les informations qui transitent sur les réseaux sont volatiles, conçues pour être transmises puis effacées, et les surveiller nécessite donc une approche proactive. De nombreux pays ont construit des centres d'analyse de données qui stockent des quantités énormes de données pendant des jours, des mois ou des années pour les analyser plus tard. Un adversaire peut aussi surveiller ton traffic réseau avec la **collaboration de ton fournisseur d'accès à Internet (#1)**, en compromettant ton routeur avec un **malware (p. 22)**, ou en surveillant tes connexions réseau filiaires ou sans fil à partir d'un véhicule de surveillance à proximité de ton domicile.

Parce que la plupart des sites web, fournisseurs d'email, et applications de messagerie utilisent le chiffrement SSL/TLS (le « s » dans « https »), un adversaire qui surveille ton traffic réseau sait généralement quels sites web tu visites, mais pas ce que tu fais sur ces sites web. Si tu utilises Tor,[12] un adversaire qui surveille ton traffic réseau sait que tu utilises Tor, mais pas quels sites web tu visites ni ce que tu fais sur ces sites web.

Tor est vulnérable aux attaques par corrélation, mais de telles attaques sont difficiles à mettre en oeuvre même pour des adversaires puissants. Les poursuites judiciaires contre le hacker anarchiste Jeremy Hammond sont un exemple d'une attaque par corrélation qui a fonctionné : les moments où le pseudonyme qu'il utilisait dans des salons de discussion était « en ligne » (obtenus par une analyse de son traffic réseau) ont été corrélés avec les moments où une opération de **surveillance physique (p. 26)** l'observait chez lui pour prouver que le pseudonyme lui appartenait.[53]

Mesures d'atténuation

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques, et en particulier utiliser Tor,[12] pour que ce soit plus difficile pour un adversaire de surveiller et analyser ton traffic réseau.

[53] https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8

- Tu peux détruire l'IMSI-catcher (les IMSI-catchers professionnels peuvent coûter très cher).

Opérations répressives

Opération contre Boris (#5) : Les enquêteurs ont utilisé des IMSI-catchers lors d'opérations de **surveillance physique (p. 26)** pour identifier les numéros de téléphone de personnes que Boris rencontrait—et ont ensuite identifié ces personnes en demandant aux opérateurs de téléphonie mobile les noms correspondant aux numéros de téléphone.[1]

Répression contre Zündlumpen (#5) : Les enquêteurs ont utilisé un IMSI-catcher pour identifier le numéro de téléphone de la mère de N. Ils l'ont utilisé à la fois au domicile de la mère et à son lieu de travail : la corrélation des deux utilisations leur a permis d'identifier le numéro de téléphone.[42]

Affaire de l'association de malfaiteurs de Bure (#5) : Les enquêteurs ont utilisé des IMSI-catchers pour identifier les numéros de téléphone de personnes qui vivaient dans des lieux en lien avec la lutte contre Cigéo ou qui participaient à des manifestations.[3]

Affaire du 8 décembre (#5) : Les enquêteurs ont utilisé un IMSI-catcher lors d'opérations de **surveillance physique (p. 26)** pour identifier les numéros de téléphone utilisés par certain·e·s des inculpé·e·s.[43]

3.20.4. Malware

Un malware est un logiciel malveillant installé sur un appareil numérique comme un ordinateur, serveur, ou téléphone portable, pour compromettre l'appareil. Les malware peuvent faire beaucoup de choses différentes, mais contre les anarchistes et autres rebelles ils visent typiquement à surveiller l'appareil compromis à distance en prenant des captures d'écran et en enregistrant le texte entré sur l'appareil, et à pister la position de l'appareil (dans le cas des téléphones).

[42] https://notrace.how/resources/fr/#gendarmes-et-voleurs

[43] https://web.archive.org/web/20241215183331/https://soutien812.blackblogs.org/2024/12/15/affaire-du-8-12-analyse-dune-enquete-preliminaire-pnat-et-dgsi

Un logiciel malveillant peut être installé sur un appareil :

- À distance, avec interaction de la cible. Cela se fait typiquement via du phishing,[44] qui nécessite souvent que la cible ouvre un fichier ou un lien malveillant.
- À distance, sans interaction de la cible. Ce type de malware est souvent très cher pour l'adversaire. Un exemple de malware qui a été capable de s'installer sans interaction de la cible est Pegasus.[45]
- En **accédant physiquement (p. 15)** à l'appareil.

Voir aussi :

- « Ça pourrait être dangereux ! Installation de logiciels espions via des attaques par ingénierie sociale en Italie »[46] pour un example de malware installé via du phishing.
- Le sujet « Logiciels malveillants ciblés ».[47]

Mesures d'atténuation

Analyse des ordinateurs et téléphones (#4) : Tu peux faire une analyse des ordinateurs et téléphones pour détecter des traces de malware sur un appareil sur lequel un malware est ou a été installé.

Bonnes pratiques numériques (#4) : Tu peux adopter de bonnes pratiques numériques pour que ce soit plus difficile pour un adversaire d'installer un malware sur tes appareils numériques. Par exemple, tu peux :

- Adopter de bonnes pratiques contre le hameçonnage (ou *phishing*) pour que ce soit plus difficile pour un adversaire de t'amener à installer un malware sur tes appareils numériques.
- Utiliser Tor[48] ou un VPN pour que ce soit plus difficile pour un adversaire d'installer un malware à distance sur tes appareils numériques via une injection réseau ciblée.[49]

[44] https://fr.wikipedia.org/wiki/Hameçonnage
[45] https://fr.wikipedia.org/wiki/Pegasus_(logiciel_espion)
[46] https://notrace.how/resources/fr/#pourrait-etre-dangereux
[47] https://notrace.how/resources/fr/#topic=targeted-malware
[48] https://torproject.org
[49] https://en.wikipedia.org/wiki/Packet_injection

Chiffrement (#4) : Tu peux chiffrer les données « en mouvement » pour que ce soit plus difficile pour un adversaire d'installer un malware via l'*injection de paquet réseau*, un vecteur d'installation pour certains malware, comme Pegasus.[50]

Cloisonnement (#4) : Si un adversaire installe un malware sur une clé USB Tails[31] ou une machine virtuelle Qubes OS[51] que tu utilises pour des identités numériques différentes, il peut relier ensemble tes différentes identités. Pour contrer ça, tu peux utiliser différentes clés USB Tails ou machines virtuelles Qubes OS pour différentes identités numériques.

Opérations répressives

Scripta Manent (#5) : Un malware a été installé sur l'ordinateur d'un·e des accusé·e·s.[52] Le malware, qui a été installé à distance par Internet, a ciblé un ordinateur Windows et était capable d'enregistrer le texte tapé au clavier, de faire des captures d'écran régulières, et d'enregistrer les communications envoyées et reçues par l'ordinateur.

Répression du sabotage de l'usine Lafarge (#5) : Les enquêteurs ont fait cinq requêtes pour installer à distance des logiciels espions.[18] Parmi celles-ci, une installation a été fructueuse (sur un iPhone SE 2020) et leur a donné accès à une conversation de groupe Signal.

Arrestation de Stecco (#5) : Les enquêteurs ont tenté d'installer un logiciel malveillant sur le smartphone d'une personne sous surveillance.[6] Ils lui ont envoyé un SMS contenant un lien. Si la personne avait cliqué sur le lien, le logiciel malveillant aurait été installé, permettant aux enquêteurs d'écouter les conversations via le microphone du smartphone. Mais la personne n'a pas cliqué sur le lien, et le logiciel malveillant n'a donc pas été installé.

[50] https://forbiddenstories.org/fr/a-propos-du-projet-pegasus
[51] https://qubes-os.org
[52] https://earsandeyes.noblogs.org/post/2019/01/27/more-precisions-keylogger-italy