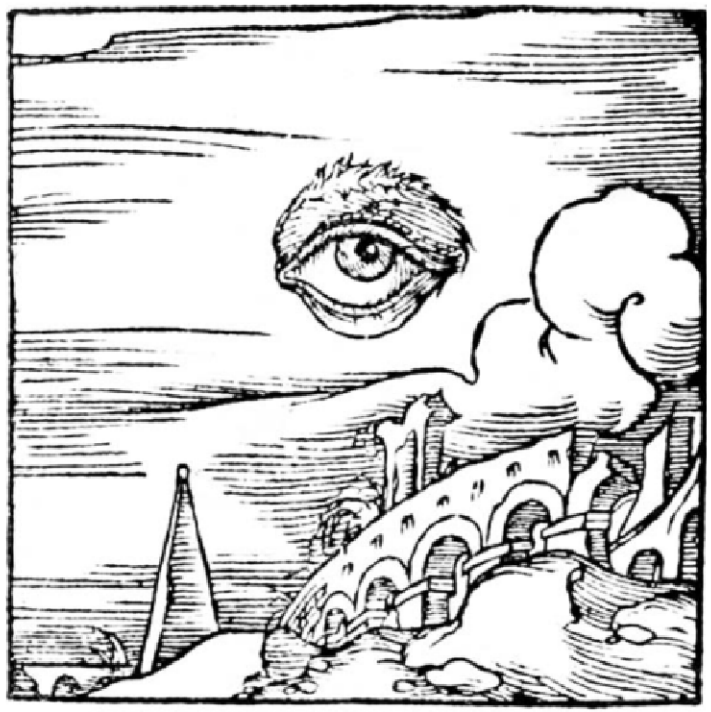
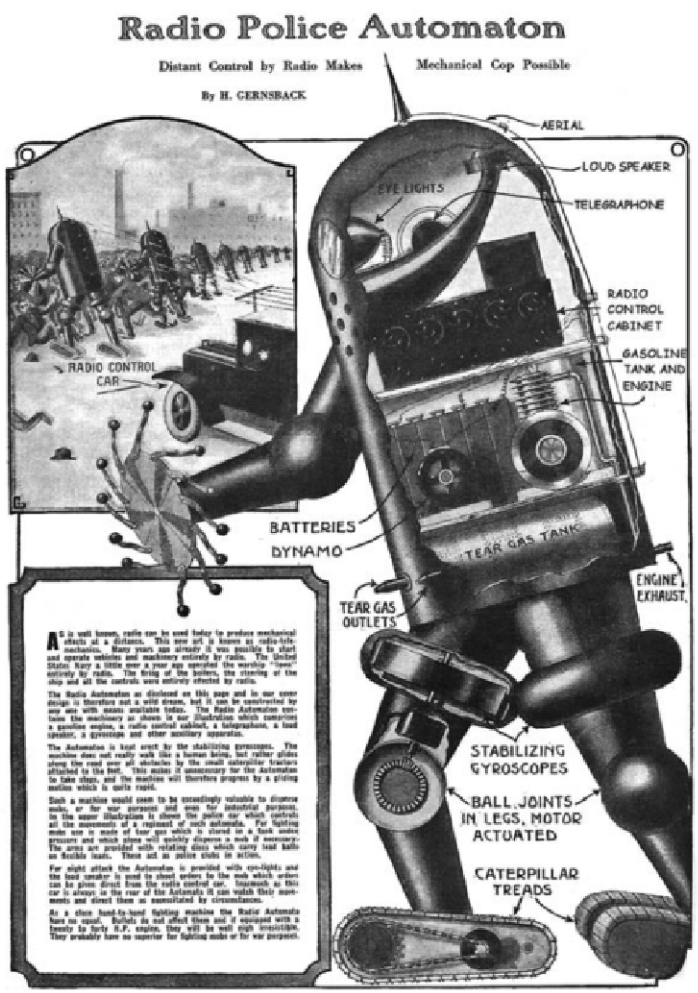
Occhi indiscreti

Relazione sulle modalità e gli strumenti di repressione digitale



arachidi@autistiche.org
arachidi.noblogs.org

Copertina: The eye of God. From Horapollo, *Ori Apollinis Niliaci: De sacris notis et sculpturis libri duo* (Paris: Kerver, 1551), 222.



A radio-controlled police automaton. From Hugo Gernsback, "Radio Police Automaton," *Science and Invention* 12, no. 1 (May 1924): 14.

protettrici della privacy. Questo, oltre ad essere evidentemente una bugia, è un fattore significativo a livello sociale, perchè esclude anche solo la possibilità di costruire, utilizzare e diffondere alternative. Il mondo che si prefigura davanti a noi diventa sempre più monolitico, con un solo binario a possibile: la sorveglianza, che sia ad opera di Microsft o degli stati.
Per questo ci viene da pensare che continuare ad usare la tecnologia a nostro vantaggio potrebbe essere un cammino scivoloso e complesso, in quanto ne abbiamo sempre meno controllo e tutte le derive sicuritare lo renderanno piu difficile.

Quali conclusioni possiamo trarre da tutto questo?
Nonostante siano possibili e siano necessarie, ciò che dobbiamo ricercare non sono soluzioni tecniche a questi giga-problemi. È ovvio che 4 scienziatx pazzx troveranno sempre il modo di aggirare questi controlli; il problema è come fare sì che non ci abituiamo, ad esempio, a fornire l'identificazione online ogni volta che ci viene chiesta, proprio come ci siamo ormai abituatx ad accettare i cookie. Non esiste un unico modo di autodifendersi tecnologicamente, nè un modo che sia definitivo e omnicomprensivo. Ogni situazione e ogni persona necessita di strumenti specifici ed equilibri singolari. Nemmeno il rifiuto totale di telefono o computer è una soluzione perfetta, perchè espone comunque ai rischi delle telecamere, dei microfoni, o banalmente richiede che altre persone intorno a noi siano disposte a fare la stessa scelta o supportarci.

Anche se questo testo voleva essere un recap di mezzi tecnici di sorveglianza, ci teniamo a ribadire che non sono gli unici strumenti di repressione.
Poichè crediamo veramente che la sorveglianza sia un problema sociale, ancor prima che tecnico, ricerchiamo e auspichiamo una continua discussione fra persone più e meno nerd, che possano con creatività aggirare i meccanismi di stato, big tech e controllo generale, compreso quello patriarcale, costruendo modi di relazionarci che ci permettano di andare al di là delle tecnologie. E questo modo, per quanto ci riguarda, deve essere esteso e diffuso al di là delle nostre bolle e delle nostre cerchie, non solo perchè la sicurezza è un problema collettivo e comunitario, ma perchè l'unica maniera per difenderci davvero è che questa cultura si diffonda e si moltiplichi, fino a quando l'ultima videocamera sarà bruciata.

La tecnologia digitale pervade ogni ambito delle nostre vite, e di certo la repressione statale delle lotte non sfugge a questa regola.

In quanto amici e compagne informatiche periodicamente siamo sottoposte a sessioni di domande su quello che sbirri e questure varie possono fare; altrettanto spesso, ci capita di essere a tiro di comportamenti che denotano una certa leggerezza, e che poco tengono conto di quanti strumenti i suddetti possano avere, e di quanto negli ultimi anni il budget destinato a strumenti di controllo all'avanguardia sia aumentato.

Per questo motivo, e per molti altri, abbiamo deciso di scrivere questo testo che raccogliesse un po' di informazioni in modo schematico su ciò che abbiamo visto o letto avvenire in questi ultimi anni.
Questo testo NON è pensato per far nascere paranoie, ma come una forma di collettivizzazione; tuttavia questa raccolta può non essere comprensiva di tutte le tecniche utilizzate dallo stato, anche perchè purtroppo della maggior parte si viene a sapere a posteriori, ossia a indagini concluse.

Per non appesantire la lettura delle amiche, lasciamo le riflessioni e analisi in fondo al documento, a disposizione di chi voglia leggerle e da cestinare per chi non voglia.

Operazioni/indagini citate:

Diana (2022):
https://ilrovescio.info/2025/06/28/sulloperazione-diana-contro-lanarchismo-in-trentino-cose-utili-da-sapere/
Scintilla (2019):
https://ilrovescio.info/2023/01/18/torino-sentenza-di-primo-grado-del-processo-scintilla/
Sismi (2022-2024):
https://ilrovescio.info/2023/07/11/le-solite/
Carnevale No Ponte (2025):
https://brughiere.noblogs.org/post/2025/09/11/sugli-arresti-moltopost-carnevale-no-ponte/
E altre di cui non ricordiamo o non c’è il nome..

0. Telecamere

0a. Telecamere Private (con microfono)

Nell'operazione a seguito del "carnevale no ponte" sulle carte si legge che sono state visionate alcune registrazioni con audio di un esercizio commerciale privato situato all'interno di un mercato coperto. Le registrazioni, secondo le carte, coprono dei punti in cui l* imputat* si riunivano e discutevano in vista del corteo, e sono dunque state utilizzate per giustificare l'accusa di premeditazione.

0b. Ti guardo il PIN dalle telecamere HD

Dal testo "Sull'operazione "Diana" contro l'anarchismo in Trentino. Cose utili da sapere" veniamo a sapere che grazie ad "una telecamera ad alta risoluzione installata all'interno dell'auto" è stato possibile leggere il codice PIN mentre questo veniva digitato sul telefono.

0c. Videocamere "video lunga distanza" con riconoscimento facciale

Nell'operazione Diana: sono state visionate videocamere con riconoscimento facciale soprattutto in luoghi di passaggio e affollati come le stazioni di treni e autobus, alla ricerca di una persona specifica. Se ci sono dei sospetti che la persona ricercata sia salita sul mezzo, vengono visionate anche le telecamere interne agli autobus.
https://irpimedia.irpi.eu/sorveglianze-viminale-riconoscimento-facciale-trasparenza/
https://www.poliziadistato.it/statics/17/lotto-2---sari-sistema-di-acquisizione-e-trasmissione-v23--

0d. Controllo delle telecamere autostradali

Durante l'operazione Sismi: per risalire a chi avesse appeso uno striscione su un ponte, hanno controllato le targhe entrate in autostrade; successivamente, hanno anche tentato di dedurre l'altezza delle persone dalle immagini acquisite. In molte operazioni gli inquirenti si servono di telecamere urbane e autostradali.

Questo testo segue un periodo abbastanza lungo di condivisione di riflessioni, chiacchiere, lettura e scrittura sulle tecnologie in generale. Per dare un quadro del contesto nel quale ci muoviamo e pensiamo, Nell'ultimo anno gli spyware sono tornati sotto i riflettori mediatici
https://www.amnesty.org/en/documents/eur70/8814/2024/en/
https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/.
In una dimensione più privata, constatiamo che aumenta sempre di più l'utilizzo di stalkerware e app di controllo parentale per fare stalking dell* propri* partner/ex. È da poco stato approvato il regolamento europeo Chatcontrol, anche se è stato rimosso dal testo l'obbligo di scansione generalizzata dei servizi di messaggistica come forma di tutela di privacy e crittografia. Questo tuttavia non ci fa ben sperare che in futuro non possa essere ripresentato nuovamente, viste le ripetute insistenze negli scorsi anni (è stato presentato per la prima volta nel 2022).
E non si tratta nemmeno "solo" di un nuovo eventuale Chatcontrol, spyware, stalkerware, intelligenza artificiale, telecamere, microfoni - e chi più ne ha più ne metta. Le recenti legislazioni (vedi articolo 13bis del decreto Caivano) puntano a restringere sempre più l'utilizzo di internet: se oggi controlli di età su siti porno (tramite verifica della carta di identità), domani sui siti che forniscono strumenti di anonimato, o che promuovono odio e violenza; banale e facile che le restrizioni si trasformino in fretta nella censura di siti di informazione e blog di vario tipo.
E non solo! A breve anche la possibilità di pubblicare e diffondere codice open source (cioè leggibile in toto e modificabile da chiunque ne abbia le capacità) sarà limitata, rendendo ad esempio impossibile diffondere applicazioni per smartphone a meno di avere l'autorizzazione di Google e Android.
Nonostante ci sembra che questi eventi rientrino perfettamente nel quadro generale di una tecnologia sempre più invasiva, controllante e repressiva, vorremmo condividere alcune riflessioni.

Nell'approfondire il mondo degli spyware nel corso di questo ultimo anno, ci siamo rese conto del fatto che le Big Tech, prima tra tutte Google (https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf), stanno costruendo una narrazione di sè come di

Non sappiamo se avrebbero collaborato, però sappiamo però che da quando Durov è stato arrestato Telegram ha aggiornato le policy sulla privacy. Possiamo verificare quante richieste sono state evase in ogni stato: ad esempio in Italia nel 2024 sono state effettuate 158 richieste che hanno impattato 419 utenti; nei primi 6 mesi del 2025, invece, 428 richieste per un totale di 1852 utenti.
Considerando l'implementazione della crittografia end to end, whatsapp "batte" telegram.
Tuttavia, Meta è stata oggetto di indagini in Italia e in Europa per questioni legate alla privacy e all'integrazione forzata della propria intelligenza artificiale nell'app WhatsApp. Inoltre di default i backup delle chat non usano crittografia.
Ogni anno Meta riceve centinaia di migliaia di richieste da parte della polizia. Non sappiamo quante ne evade, ma sappiamo che tipo di dati possiede: numero di telefono, durata dell'attività, tempi di connessione, uso dell'account e metadati dei messaggi e chiamate.
https://te-k.github.io/telegram-transparency/

Come ci proteggiamo?

Più info su app di messaggistica ->
https://cloud.systemli.org/s/cmJzEFXHqjwLs39
Per noi l'opzione migliore, quella cioè che garantisce il miglior equilibro fra sicurezza, facilità di utilizzo e diffusione rimane al momento ancora Signal, ma ci sono tante app che garantiscono l'anonimato che sono utilizzabili all'occorrenza.
https://www.anarsec.guide/posts/e2ee/

---

4. Varie

4a. Controllo dei movimenti bancari

È un'operazione comune a diverse indagini; è stata utilizzata ad esempio per verificare l'esistenza di movimenti sospetti in appoggio alla latitanza, oppure per verificare quali movimenti fossero legati a casse di solidarietà per l* prigioner*.

---

1. Telefoni

1a. Estrazione Forense - Attacco Locale

Un caso specifico riguarda tre telefoni sequestrati il 20 marzo 2024 durante un'azione all'aeroporto di Malpensa. Gli smartphone, protetti da PIN e con crittografia attiva, sono stati riconsegnati con chiari segni di compromissione: due di essi avevano i PIN scritti su un adesivo sul retro, un'indicazione evidente che erano stati sbloccati e analizzati.
A quanto ci risulta i dispositivi erano spenti e relativamente aggiornati, richiedendo uno sblocco da telefono spento, che nei termini stessi di Cellebrite è definito *Before First Unlock* (BFU), tecnicamente tra i più complessi da sviluppare e costosi da acquisire.

Come ci proteggiamo?

Purtroppo la sicurezza dei dispositivi mobili è legata al modello e all'aggiornamento (anche hardware), che alle volte può essere proibitiva.
Esiste un progetto opensource Graphene OS che fa un grande lavoro di messa in sicurezza ma occorre avere un telefono specifico (a novembre 2025 il modello più economico è il Google Pixel 6, circa 100 euro).
Per tutti gli altri modelli (del mondo android) non esistono soluzioni economiche e sicure. Esistono però alcune soluzioni più economiche e accessibili per cancellare tutti i dati in caso di compromissione, nello specifico app scaricabili da un app store alternativo (chiamato Fdroid), che permettono la cancellazione dei dati in caso qualcuno tenti di entrare nel telefono senza consenso.
Per approfondimenti vedi apps come Wasted, Duress.
https://search.f-droid.org/?q=wasted&lang=en
https://osservatorionessuno.org/it/blog/2025/03/cellebrite-e-luso-ordinario-della-sorveglianza-digitale-in-italia/
https://nocprtorino.noblogs.org/post/2025/02/11/da-malpensa-a-tel-aviv-come-le-aziende-di-sicurezza-informatica-israeliane-collaborano-con-le-autorita-italiane-per-accedere-ai-dispositivi-mobili/
https://www.anarsec.guide/posts/grapheneos/

1b. Utilizzo della procedura preview

A telefono sbloccato, viene visionato manualmente il contenuto del dispositivo (chat, foto) registrando schermo e audio.

Come ci proteggiamo?

Non dare il PIN: in Italia è legale (non che sia una garanzia), dimenticarselo quando te lo chiede la polizia è cortesia.
Controlla bene come fare se ti trovi in altri Stati e sappi che a seconda del reato possono giustificare un sequestro, verifica cosa puoi fare perchè la legislazione cambia da paese a paese.
Inoltre considera che avere un PIN corto o un PIN come "1312" equivale a darlo di propria sponte.
La lunghezza consigliata è sulle 8-10 cifre composta da caratteri alfanumerici.
https://archerpoint.com/wp-content/uploads/2025/06/blog-2025-cybersecurity-brute-force-update-01.jpg

1c. Localizzazione (Tramite le celle telefoniche)

Vengono spesso citate due modalità di ottenere la localizzazione dei cellulari tramite le celle: traffico aggregato e traffico disaggregato.
Nel primo caso, l'operatore telefonico fornisce la cella di aggancio (cioè quella a cui si collega il telefono quando ci si connette a internet); tuttavia, a meno di eventi come perdita di segnale, spegnimento del telefono, aggancio ad una wi-fi, non si vedono le celle di transito (cioè quelle a cui si collega il telefono mano a mano che ci si sposta) e dunque non è possibile dedurre con precisione gli spostamenti.
Questo si risolve con il traffico disaggregato, perchè permette di visualizzare anche celle di transito e di sgancio (cioè quella in cui ci si disconnette).
Non abbiamo trovato traccia, nelle carte analizzate, di traffico disaggregato, immaginiamo che in alcuni casi e alcuni provider possano fornirlo.

Come ci proteggiamo?

A seconda del proprio modello di rischio sarà utile valutare se tenere il telefono a casa o portarlo in modalità aereo.
Anche non portare il telefono può essere considerato un aggravante.

ProtonMail è considerata, e si propone, come un'alternativa valida e privacy oriented ma è bene ricordare che nel 2020 la società ha fornito informazioni sull'indirizzo IP di un account legato ad un attivista per il clima francese, che è stat* poi arrestat*.
Nello stesso anno, Proton Technologies ha ricevuto 3572 ordini dalle autorità svizzere di condividere informazioni sugli utenti, rispetto ai 13 del 2017. Dei 3572 ordini ricevuti, 195 erano richieste provenienti dall'estero. L'azienda ha contestato 750 ordini e soddisfatto 3017 richieste.
Ricordiamo sempre che queste aziende non possono fornire dati che non hanno! ;)
https://proton.me/blog/climate-activist-arrest
https://transparencyreport.google.com/user-data/overview?hl=it

ID GAIA

Op Diana: viene segnalata l'analisi dell'ID GAIA (Google Account and Id Administration); quando si cerca di collegarsi a Gmail da un dispositivo differente dal solito, viene richiesta un'ulteriore verifica tramite sms. Dato che un numero collegato all'utente riceve questo codice, chi svolge le indagini cerca dati relativi a quell'account. Avendo ottenuto l'ID GAIA di questo account, tramite l'url https://google.com/maps/contrib/IDGAIA visualizzano tutte le recensioni lasciate da quell'account risalendo così alle mail collegate. Richiedono a Google i file di Log di ogni connessione all'account. Non sembra che abbiano avuto risposta.
In sostanza, ad ogni ID GAIA possono essere associati più indirizzi email e più numeri di telefono di riferimento, una volta che la polizia conosce uno di questi dati può provare a risalire agli altri.

3c. Monitoraggio di social e blog d'area

Già, sembra che li seguano come una soap opera... Sono sicuramente più informati di tutt* noi.
In varie carte ne citano il monitoraggio continuo.

3d. Chat di Whatsapp e Telegram

Op Diana: sebbene non ve ne sia poi traccia nelle intercettazioni, in più punti la Digos chiede l'autorizzazione per scaricare le chat di Whatsapp e in un caso anche di Telegram.

Come ci proteggiamo?

Anche in questo caso l'utilizzo della rete TOR o di una VPN avrebbe reso le indagini molto più complicate per gli inquirenti, inoltre è possibile nascondere su wordpress i nomi di chi carica gli articoli.

3b. Occhio ai metadati e i servizi che usiamo!

Meta può fornire l'account che ha creato una determinata pagina o gruppo.

Nell'operazione Scintilla è stata utilizzata come prova la gestione di una pagina Facebook, che è stata messa in relazione ad alcune persone tramite gli indirizzi mail associati agli account che hanno creato o gestiscono la pagina.
Successivamente, è stata fatta una richiesta a Google per ottenere gli indirizzi IP legati alla email.
L'indirizzo IP è stato poi associato a un utenza grazie alla collaborazione del provider telefonico.

Come ci proteggiamo?

Usare provider di mail (https://riseup.net/en/security/resources/radical-servers) che non collaborano con forze dell'ordine o utilizzare sistemi per mascherare il proprio IP (Tor,VPN,Proxy)

Ma Gmail, Microsoft, Meta, Proton etc forniscono sempre le informazioni richieste?

Op Diana: in seguito ad un'intercettazione ambientale in cui viene nominato un indirizzo email, chiedono a Microsoft l'anagrafica, i dati fatturazione dell'account (nel caso in cui siano stati effettuati acquisti su Microsoft Online Store), i log delle connessioni IP, tutti gli indirizzi email e i numeri di telefono associati a tale indirizzo e tutti i soggetti che si sono registrati con un nome collegato a quell'email. Inoltre chiedono al provider subito.it il tabulato dei file di Log e degli indirizzi IP utilizzati da questa email.
Nonostante la collaborazione fra provider italiani e forze dell'ordine sia appurata e matematica, non possiamo dire lo stesso per le bigtech.

2. Intercettazioni mirate

2a. Chiamate "Normali" e SMS

Ricordiamoci che abbiamo sempre qualcosa da nascondere, perchè ogni informazione può essere preziosa al momento delle indagini, non possiamo prevedere cosa verrà usato contro di noi, e l'analisi del traffico in chiaro è molto facile e poco costosa.
La conservazione dei dati dei provider telefonici avviene secondo quanto previsto dall'articolo 132 del Codice della Privacy e dalle normative di Data Retention, con alcune specifiche differenze in base al tipo di dato:

- dati relativi al traffico telefonico (Non il contenuto delle chiamate, ma quanto, quando e chi): conservati per 24 mesi dalla data della comunicazione.
- dati relativi al traffico telematico (esclusi i contenuti delle comunicazioni, come dati di connessione a internet o SMS): conservati per 12 mesi.
- dati relativi alle chiamate senza risposta: conservati per 30 giorni.

Alcune leggi recenti hanno discusso l'estensione fino a 6 anni per motivi di sicurezza, la conservazione riguarderebbe anche i dati di collegamento a celle telefoniche, che rientrano nel traffico telematico.
Nell'operazione Diana è stata anche presa visione dei tabulati delle cabine telefoniche.

Come ci proteggiamo?

Non usando chiamate ed sms!
Ma utilizzando app di messaggistica cifrate come Signal, ne parliamo meglio nella sezione 3d.

2b. Intercettazione Telematica Passiva - Attacco Remoto

Op Sismi: nei listini prezzi l'intercettazione telematica passiva (nel 2022 risulta costare 30€ al giorno) è descritta come "intercettazione passiva del flusso dati telematico relativo a utenze fisse ADSL o mobili (trasmissione dati in 2G, 3G, 4G) per i Gestori che provvedono in autonomia alla cattura dei dati".
Se invece il gestore non effettua questo servizio ha un costo di 60€ al giorno.
In sostanza permette di visualizzare il traffico dati, ad esempio richieste DNS, i siti visitati, la versione del sistema operativo corrente, la presenza di antivirus, le app installate e le abitudini nell'utilizzo del dispositivo da parte dell'utente.
Nel listino prezzi del 2023 viene ampiamente sottolineato come questo tipo di intercettazione sia funzionale all'intercettazione telematica attiva (infezione con spyware), sia perchè per infettare un dispositivo bisogna conoscere le abitudini di chi lo usa, sia per capire se effettivamente sia necessario procedere con un'infezione (ben più costosa).

Come ci proteggiamo?

Utilizzare la rete TOR (https://www.torproject.org/) o una VPN renderà cifrate le informazione citate sopra.

Per l* più curios*:

Bisogna comunque prestare attenzione però alle varie sfumature, ad esempio se utilizzassimo Tails da una rete sotto intercettazione (che sia di casa o di un hotspot) non sarà possibile visualizzare alcun tipo di traffico in chiaro (se non che sta venendo utilizzata la rete Tor); se invece utilizzassimo il TorBroswer ovviamente solo i siti visitati tramite quell'applicazione saranno protetti da occhi indiscreti.
Sarà importante verificare che i DNS server utilizzati siano verso il tunnel crittografato della VPN e che in caso di smartphone tutto il traffico passi effettivamente esclusivamente per la VPN.

una SIM per la trasmissione e una memoria interna o microsd per salvare le registrazioni.
https://hackrf.readthedocs.io/en/latest/hackrf_one.html
https://www.notrace.how/earsandeyes/#

3. Blog, social e varie

3a. Attacco al sito web

In delle carte giudiziare si legge: “attività mirata con tecniche di OSINT ed Ethical Hacking diretta ad analizzare la struttura della piattaforma… per evidenziare vulnerabilità utili ad una successiva ‘intrusione’”. Non viene detto che l’intrusione sia realmente avvenuta, ma che era autorizzabile “qualora” fosse stato necessario.

Ciò che è avvenuto proviamo a descriverlo qui sotto brevemente.
La polizia ha:

1. Effettuato analisi OSINT su sito e contenuti (Ricerca di informazione pubbliche sul blog e la sua infrastruttura)

2. Identificato i nomi e nickname di chi ha scritto gli articoli (sempre un informazione pubblica, nascondibile su wordpress(!))

3. Raccolto i dati su utent* che lo visitavano chiedendo al provider del sito web (Aruba, Hostinger, etc) dei log di accesso.
Ottenuto gli indirizzi IP che hanno visualizzato la pagina in certi orari (i dati sono stati consegnati dal provider senza avvisare chi gestiva il sito).

4. Richiesto all’ISP (Fastweb,Tim, Vodafone etc) di identificare gli IP associandoli ad un'utenza (intestatario, indirizzo).

5. Correlato i dati con intercettazioni telefoniche e altri tabulati per rafforzare l’attribuzione degli articoli ad una persona specifica.

6. Ottenuto autorizzazione di eventuale analisi tecnica del sito (ricerca di vulnerabilità) per valutare possibilità di intrusione o per acquisire ulteriori prove tecniche.

2d. Imsicatcher - Celle Telefoniche "Spia"

Un IMSI catcher simula una torre cellulare, inducendo i telefoni vicini a collegarcisi. Così può intercettare IMSI, IMEI, chiamate, messaggi, dati di localizzazione e traffico internet, oltre a permettere attacchi man-in-the-middle. Non ci sono prove del suo uso, ma potrebbe servire per intercettazioni e deviazioni di traffico. In Italia risultano bandi di Polizia di Stato e Guardia di Finanza per IMSI catcher mobili e fissi.

Come ci proteggiamo?

Alcuni telefoni consentono di disattivare le chiamate 2G dalle impostazioni di rete, riducendo il rischio di intercettazioni non autorizzate. In ogni caso, un dispositivo acceso con o senza sim e non in modalità aereo si collega comunque a una cella telefonica, rendendo possibile la localizzazione.
https://www.lanotiziagiornale.it/tempi-duri-per-gli-evasori-la-guardia-di-finanza-acquista-gli-imsi-catcher-per-rintracciare-i-cellulari/
https://efforg.github.io/rayhunter/

2e. Microfoni ambientali direzionali

Se le guardie conoscono i luoghi abituali delle riunioni, possono installarvi videocamere-microfoni. Anche cambiando posto, non è sempre facile accorgersi di essere seguit*, quindi è fondamentale verificare la sicurezza dei luoghi di incontro e verificare se sia possibile l'utilizzo di un direzionale. In diverse indagini sono state trovate microspie, con microfono o GPS, in auto, abitazioni o persino biciclette.

Come ci proteggiamo?

Per individuare microspie è preferibile una ricerca manuale, poiché gli strumenti tecnologici sono spesso costosi o poco efficaci. In auto si trovano di solito collegate alla batteria e nascoste nell'abitacolo; in casa vicino alle prese o dentro elettrodomestici come frigo e microonde. Esistono anche versioni a batteria per intercettazioni brevi, più difficili da scoprire. Spesso includono

2c. Intercettazione Telematica Attiva - SPYWARE

Disclaimer

I casi che abbiamo potuto analizzare si basano tutti su smartphone, ma potrebbero essere installati anche su pc con tecniche simili; inoltre le tecniche di attacco potrebbero essere oggi diverse e più sofisticate.

Op Sismi: avvenuta infenzione di un dispositivo tramite uno spyware di stato dal nome "Spyrtacus".
Questa al momento è la terza volta che accade nel corso degli ultimi anni (da quel che ne sappiamo) e alcune parti dell'attacco accomunano tutti i casi che abbiamo potuto studiare.

Come avviene l'infenzione?

La collaborazione del provider telefonico e la creazione di attacchi di phishing costruiti su misura sono vitali.
Lo studio del target, che può essere più o meno approfondito, avviene tramite le intercettazioni telefoniche classiche oppure attraverso l'intercettazione telematica passiva citata sopra.

La procedura standard più utilizzata è la seguente:

1. Viene interrotta la connettività dati e telefonica al dispositivo sotto attacco, se necessario per giorni.

2. Per ottenere spiegazioni, l'utente sotto attacco a questo punto chiama l'assistenza volontariamente, oppure tutte le chiamate in uscita vengono reindirizzate automaticamente all'assistenza. In realtà, verremo mess* in contatto con un reparto tecnico che si occuperà invece di installare il malware.

3. Il reparto tecnico chiederà all'utente sotto attacco di installare un'applicazione non dal playstore ma da un sito, all'apparenza legittimo, che potrebbe anche essere inviato tramite sms col numero del provider telefonico. Si verrà guidat* ad approvare i permessi necessari per l'installazione ed il corretto funzionamento dell'applicazione (come installare app da fonti sconosciute, abilitare che l'app giri in background, escluderla da controlli google playprotect, microfono, posizione etcetc).

Durante l'op. Sismi, invece, hanno preferito fingersi di Trenitalia e con qualche promessa hanno convinto ad installare l'applicazione malevola.

È possibile che utilizzino altri metodi per installare uno spyware?

Esistono metodi più costosi e più efficaci per l'installazione, ad esempio con un attacco oneclick (un messaggio con un link malevolo, un pdf oppure un file excel che se cliccato installerà in maniera nascosta uno spyware senza che la persona si accorga di niente).
Attacchi ancora più costosi e sofisticati detti zeroclick dove non è necessaria nessuna interazione utente, come avvenuta per il famoso caso dello spyware "Graphite" dell'azienda "Paragon Solutions", o qualche anno indietro per "Pegasus" di "NSO Group".
È possibile che vengano installati, a seguito di un sequestro di Polizia più o meno lungo, nonostante in Italia non ne abbiamo ancora evidenze.
https://www.amnesty.it/serbia-ecco-come-attivisti-e-giornalisti-indipendenti-vengono-spiati/
https://decripto.org/caso-paragon-analisi-dello-spyware-graphite-e-come-ha-infettato-i-telefonini-di-giornalisti-e-attivisti/
https://brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso/
https://techcrunch.com/2025/02/13/spyware-maker-caught-distributing-malicious-android-apps-for-years

Cosa può fare uno spyware di solito?

- attivare il microfono da remoto
- leggere notifiche
- vedere lo schermo in tempo reale
- effettuare screenshot
- verificare la posizione precisa
- potenzialmente un controllo compleso del dispositivo
- Pagando ulteriormente è possibile avere accesso ad app di messaggistica come Whatsapp, Telegram e Messenger, ma non c'è traccia che sia effettivamente avvenuto.

Come ci proteggiamo?

Non dobbiamo sottovalutare gli attacchi di Phishing perché, quando è confenzionato a misura su di noi, cascarci è molto più facile di quello che pensiamo.
Prendendo come esempio il caso che riguarda trenitalia, sarebbe stato così strano se durante la chiamata vi avessero citato tutti i vostri ultimi viaggi, dando così prova della loro affidabilità? Se la chiamata fosse arrivata subito dopo l'acquisto di un biglietto?
Se la chiamata arrivasse in un momento in cui le difese sono basse e suonasse tutto cosi plausibile cascarci non sembra poi così improbabile.
Anche in questo caso sistemi operativi come Graphene OS ci proteggono maggiormente, ma non cliccare su link strani e non fidarsi di assistenze campate per aria sono la nostra prima difesa.

Come facciamo a capire se un telefono è infetto?

L'applicazione può essere nascosta o fingersi altro, ma probabilmente userà tantissima batteria e come detto sopra la installeremo di "nostra volontà", quindi basterà ricordarsi se siamo stat* guidat* ad installare una qualche applicazione di recente.
In caso dovessi notare qualche segno di tentativi di infezione o se il telefono è stato sequestrato dalla polizia, esiste una rete di persone che ha l'interesse nell'analizzare telefoni che potrebbero essere stati compromessi che puoi contattare tramite la mail: "cispiano@anche.no". Contattate anche il vostro hacklab di fiducia (perchè ne avete uno vero?)!

È possibile che lo spyware sopravviva ad un reset di fabbrica?

Tendenzialmente no.

È possibile che lo spyware sopravviva ad un riavvio?

Tendenzialmente sì.