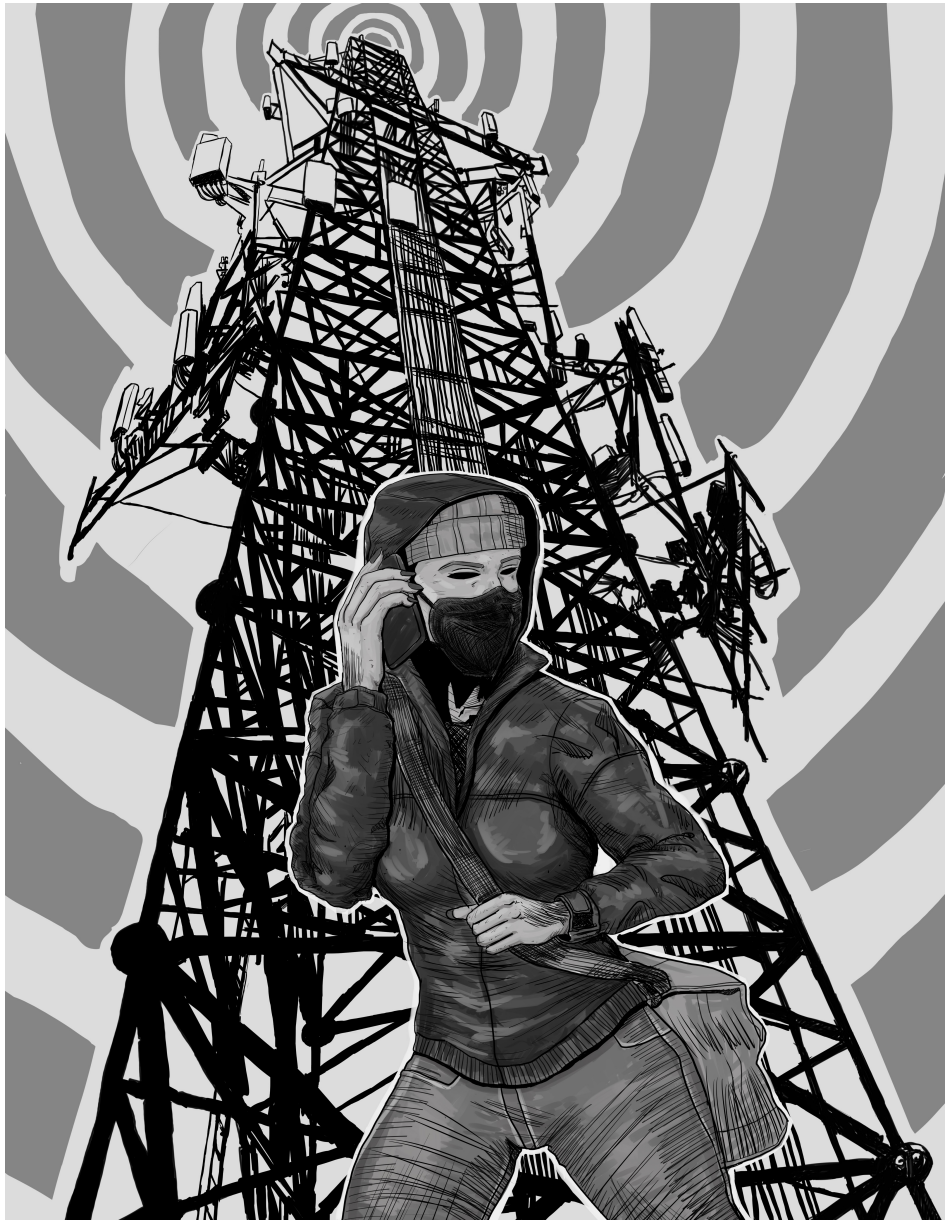
SICUREZZA DEI TELEFONI

PER SITUAZIONI DI ATTIVISMO E AGITAZIONI



HÅKAN GEIJER

TRADUZIONE A CURA DI DEL GRUPPO TRADUZIONE TELEFONI SICURI

esterne è chiamato nichilismo della sicurezza. Chi ragiona così di solito prende una di queste due strade: o pensano che nessuna contromisura è efficace, quindi non prendono nessuna precauzione e creano una sorta di profezia che si autoavvera con il proprio arresto; oppure credono nel supremo dominio dello Stato e finiscono paralizzati nell'inattività. La repressione non funziona solo grazie ai manganelli che ci colpiscono o alle prigioni che ci ingabbiano, ma anche grazie alla paura della sanzione e della nostra conseguente immobilità autoimposta. Ogni piccolo accorgimento che prendi può proteggerti, e molti di questi sono così semplici che puoi cominciare ad applicarli ora. Come cosa più facile, puoi evitare la rete della sorveglianza usando delle semplici app di messaggistica crittografate e lasciare il telefono a casa durante manifestazioni e azioni. Ogni passo oltre questi richiederanno alla controparte uno sforzo maggiore e più mirato se vogliono controllarti o arrestarti. Il tempo e le risorse sono limitate anche per gli istituti di sorveglianza. Gli esseri umani fanno errori e i computer si rompono. I tuoi avversari non sono infallibili e tu puoi diminuire notevolmente la quantità di dati che possono raccogliere e che tipo di conoscenza ne possono trarre.

In più, lo Stato non usa sempre il massimo dei suoi possibili sistemi di controllo. Solo perchè lo Stato ha l'effettiva possibilità di violare o tracciare il tuo telefono, sicuramente non lo fa per beccarti che passeggi in un parco dopo il suo orario di chiusura. Anche in casi in cui lo Stato vuole usare al massimo i sistemi di controllo può capitare che lo faccia male. Il tuo modelo di rischio dovrebbe tenere in conto una risposta verosimile dalla controparte in base alle informazioni che ha su di te. Prova a capire come si muove la polizia, i fascisti e altri nemici nella tua zona e formula un modello di rischio per te e il tuo giro. Discutine a lungo con compagni e compagne. Conincia con un po' di strategie di sicurezza fino a renderle una vera e propria cultura della sicurezza. Condividi conoscenza e pratiche che portano a un maggiore livello di sicurezza contro i pericoli che è probabile incontrare. Fai dei passi concreti e tangibili. Comincia con calma con un paio di cose alla volta finchè vengono interiorizzate come routine, per poi proseguire. Un piano di questo tipo funziona solo se si mette in pratica, e andare di fretta con un sacco di cambiamenti in un gruppo rischia di essere un sovraccarico eccessivo e portare a frustrazione. Meglio andare per gradi.

Occhio alle leggende metropolitane. Gli spazi di movimento ne sono pieni, e la sicurezza non fa eccezione. Chiedi "come?" e "perchè?" quando la gente fa dichiarazioni su controllo e contromisure. Basa il tuo modello di rischio e i tuoi piani di sicurezza su fatti verificati—o almeno congetture molto realistiche e supportate da qualche tipo di prova. Usa queste conoscenze per proteggere te e chi ti sta intorno mentre lottate insieme.

Caso 9: gestire un anello debole

Scenario

Un gruppo di affinità si occupa di contrastare i nazi che creano problemi ad alcune persone della loro comunità. In questo gruppo la regola è non portare il telefono alle azioni notturne. Felix, uno dei membri più attivi, pensa che sia una paranoia eccessiva e si rifiuta di lasciare il suo a casa.

Premesse

Il gruppo ritiene che lo Stato possa usare la posizione dei telefoni per indagini sulle sue attività. I membri pensano anche che Felix metta in pericolo il gruppo portandosi dietro il telefono.

Contromisure

Per evitare che Felix metta in pericolo tutti e tutte, il gruppo ha temporaneamente sospeso le attività finché non si troverà un accordo con Felix.

Analisi

Le azioni di Felix mettono davvero a rischio il gruppo, ed è sensato non farlo partecipare alle azioni. Se il gruppo stoppa del tutto le azioni, però, questo può nuocere alla comunità, e il rischio di essere arrestati per i telefoni può variare a seconda di come si muove la polizia nel paese o nella regione in questione.

Consigli

Il gruppo di affinità può creare un sottogruppo di persone che sono d'accordo a non portarsi il telefono durante le azioni e continuare il proprio lavoro. In parallelo, può fare un percorso con Felix per fargli capire come e perché portarsi il telefono crea un rischio non necessario. Possono discutere con lui del fatto che il suo comportamento mette il resto del gruppo a disagio e che le conseguenze di questo non ricadono solo su di lui. Il gruppo può riuscire a rimanere affine a Felix ma può aver bisogno di escluderlo dalle azioni più rischiose se si rifiuta di lasciare il telefono a casa.

Considerazioni finali

La tecnologia non è buona o cattiva—per lo meno una buona parte. Non significa né emancipazione né oppressione di per sé. Le nuove tecnologie creano nuove opportunità mentre ne eliminano altre. Stessa cosa vale per i telefoni. Avere accesso a comunicazione istantanea e conoscenza illimitata comodamente nelle nostre tasche è spaventosamente potente, ma va di pari passo con un aumento del controllo.

Puoi pensare che lo Stato non ti stia sorvegliando, ma se fai parte dei movimenti—anche nel giro largo—in realtà sicuramente lo fa. Proteggerti può proteggere i tuoi amici, la tua famiglia, i compagni e le compagne che sono più coinvolte nel movimento. Puoi pensare che lo Stato stia spiando il tuo telefono per ascoltare le tue assemblee di condominio, ma molto probabilmente non è così. La sicureza assoluta in ogni momento è irraggiungibile, e provarci è gravoso.

Dopo aver letto queste pagine potrebbe venirti da dire "ma mi tracceranno comunque". Pensare che non è possibile avere un livello di sicurezza contro le minacce

Introduzione

Alcuni dei più importanti strumenti a nostra disposizione sono i nostri telefoni sempre connessi ad internet. La comunicazione istantanea e la somma di tutta la conoscienza umana a disposizione di un tocco ha incredibilmente cambiato la possibilità di influenzare e farci influenzare dal mondo. Ma questa costante connessione ha un prezzo, e lo paghiamo con il costo della crescente sorveglianza degli Stati e delle aziende private di sorveglianza. Coloro che sono attivi in movimenti libertari sono a conoscenza dei vari livelli di sorveglianza e collettivamente hanno sviluppato un modello di sicurezza operazionale (OpSec), ovvero un insieme di pratiche e cultura alla sicurezza per contrastare i tentativi di chi vuole ostacolare un' organizzazione.

Ci sono molte leggende metropolitane sui cellulari che provengono da un' incompleta comprensione della tecnologia usata dai telefoni alla base e quali caratteristiche lo stato e i settori privati hanno a disposizione per sorvegliare le persone usando i loro telefoni. Il Modello di rischio è il processo base per identificare le minacce e costruire contromisure specifiche e pragmatiche contro questi avversari, ma senza un modello chiaro di funzionamento di tali avversari si rischia di usare contromisure inefficaci. Azioni basate sulla disinformazione possono portare ad arresti immediati o creare l'impressione di un avversario che vede tutto, soffocanto così l'azione. Questo testo prova a coprire le tecnologie alla base di un telefono e sfatare certe leggende metropolitane così che tu e le persone tue complici possiate resistere e organizzarvi efficacemente.

Non esiste una cosa come la sicurezza perfetta, non è una cosa binaria che si può "accendere" o "spegnere", non esiste nemmeno uno spettro di "miglior sicurezza" o "peggior sicurezza". La sicurezza ha senso se discussa in termini di "miglior sicurezza sotto certe condizioni con problemi e minacce particolari". Quello che può essere efficace per evitare che lo stato di sorvegli potrebbe non essere il miglior modo per evitare che il tuo partner abusivo controlli i tuoi spostamenti e le tue conversazioni. Questa guida vuole metterti a conoscenza delle possibilità e dei rischi così che tu prenda la decisione migliore in ogni situazione. La cultura alla sicurezza non è una garanzia di sicurezza, ma riduce i possibili danni. Può evitare che ti arrestino o salvare la tua vita o quelle delle persone accanto a te.

Questo testo è stato scritto all'inizio del 2022 e tradotto a inizio 2023 da alcuni anarchici e anarchiche che risiedono in europa, in nord america e la maggior parte di ciò che sarà scritto riteniamo sia più utile per le persone che condividono gli stessi spazi e lo stesso tempo. Abbiamo intenzionalmente omesso la maggior parte delle considerazioni legali; considerato che anche se i nostri avversari non sono autorizzati a fare certe cose poi le fanno lo stesso. Abbiamo preferito concentrarci su ciò che è tecnicamente possibile. Riconoscendo e migliorando anche grazie a quelli che sono gli errori che non abbiamo visto anni fa (e nuovi errori disponibili in questo testo), ma non siamo in grado di predirre il futuro. Quindi ti consigliamo di usare la tua conoscienza del contesto locale per adattare ogni dettaglio qui scritto alle minacce che affronterai direttamente.

Tu e il tuo telefono

Il tuo telefono[1] non è semplicemente un costoso oggetto personale. È un'estensione della tua persona. Contiene i tuoi ricordi, le tue conoscenze, i tuoi pensieri privati e semi-privati. Ti permette di trovare velocemente informazioni e condividerle con altri. Questa connessione e accesso alla conoscenza ci rende più efficaci nel raggiungimento dei nostri obiettivi. I telefoni—in un certo senso—sono diventati requisiti necessari per poter funzionare nella nostra società moderna. Per questa ragione, le persone non ne sono quasi mai prive. Quando muore la batteria o dimentichiamo il telefono a casa, ci sentiamo nudi, inabili, o come se una parte di noi mancasse.

La compromissione di un dispositivo da parte di un avversario, sia essa in seguito a un sequestro o un'infezione di malware, può avere conseguenze disastrose. Tutte le tue foto, messaggi di testo, email e note potrebbero essere accessibili all'avversario, così come gli accessi a tutti gli account su cui si è temporaneamente loggati dal propio telefono. Malware o applicazioni per lo stalking potrebbero attivare il microfono dello smartphone o il tracciamento real time dei tuoi spostamenti anche dopo che il telefono ti sia stato restituito.

Oltre a questi tipi di sorveglianza attiva, il tuo telefono fornisce informazioni per la sorveglianza passiva ad avversari con una posizione privilegiata, quali la polizia che può richiedere l'accesso ai metadati posseduti dal tuo ISP[2] o dalla tua compagnia telefonica, sia real-time che al loro archivio.

È per queste ragioni che gli attivisti dicono "Il tuo telefono è uno sbirro" o "Il tuo telefono è una spia". Detto questo, dovremmo continuare a usare i nostri telefoni per i vantaggi che il loro uso comporta o dovremmo abbandonarli per i rischi che portano con sé? Esistono degli accorgimenti su come e quando usare i telefoni che possono permetterci di sfruttare molti dei benefici che comportano, evitando la maggior parte degli svantaggi.

Telefoni e tecnologie

Per capire come i telefoni possono essere manomessi e usati per agevolare la sorveglianza, abbiamo bisogno di sapere in maniera precisa in che modo funzionano le varie tecnologie che si usano dentro, come ad esempio cosa c'è dentro (hardware), come ci si parla con quello che c'è dentro (firmware), come farci girare delle app (sistema operativo), e quindi le reti cellulari considerando in generale anche come funziona internet in un telefono. Questo ci aiuterà a costruire un modello di rischio adatto a noi, così da poter prendere decisioni consapevoli valutando rischi e probabilità.

[1] Per comodità, con telefono si intende "telefono cellulare" o "smartphone"

[2] Internet service provider

corpose dovrebbero stare fuori dalle email perchè queste sono tutte informazioni che danno allo Stato una panoramica dettagliata del collettivo e possono essere usate contro di esso.

Caso 8: i rave

Scenario

Un collettivo organizza rave illegali all'aperto durante la pandemia di Covid. Chiedono a chi partecipa di indossare le mascherine e pensano che questo sia un livello di sicurezza sufficiente contro la diffusione del virus. La polizia ha dato il divieto assoluto di assembramenti (tranne che per il lavoro e altri ingranaggi della macchina capitalistica).

Premesse

Lo Stato mette molte energie nell'evitare assembramenti (certo, solo quelli sgraditi), ma probabilmente non farà sforzi retroattivi per indagare su assembramenti passati. Le forze dell'ordine hanno la possibilità di raccogliere dati sulla posizione dei telefoni in tempo reale e può usarli per scovare se centinaia di persone si sono radunate in qualche posto remoto. La polizia ha informatori che seguono questo tipo di eventi, e ad alcune persone piace fare la spia se sentono cose non di proprio gradimento.

Contromisure

Il rave non viene pubblicato sui social, e si chiede che le info siano solo inoltrate ad altri contatti con mezzi sicuri. Nelle info è richiesto alle persone di mettere il telefono in modalità aerea quando si avvicinano vicino alla location.

Analisi

Non pubblicizzare l'evento sul social ovviamente è un passaggio corretto per evitare che la polizia ne venga a conoscenza automaticamente. Chiedere di diffondere le info a contatti fidati in modi sicuri è un ottimo modo per ridurre il rischio, ma basta che una sola persona mandi il messaggio solo con luogo e data per perdere l'avviso per strada. Anche se il collettivo lo sa, è un rischio che ritiene accettabile.

Consigli

C'è poco da fare per evitare che la gente arrivi col telefono acceso, e poco si può fare per assicurarsi che il messaggio-info rimanga su canali fidati e con un occhio alla sicurezza. Questo è un grande problema nella cultura della sicurezza perchè la mancanza di un buon livello di sicurezza da parte di alcune persone può avere ripercussioni su tutto il gruppo, soprattutto dal momento che il beneficio individuale di tenere il telefono acceso e alto ma il rischio individuale è basso. Chi organizza e porta la strumentazione è chi più probabilmente deve affrontare le conseguenze. Infatti se i partecipanti si disperdono durante un blitz della polizia, probabilmente eviteranno le conseguenze legali. La cosa migliore che il collettivo può fare è convincere le persone prima e durante il rave del fatto che le loro azioni possono essere responsabili delle sorti del rave per tutti e tutte.

Caso 7: organizzazione generica e comunicazioni

Scenario

Un collettivo organizza proteste in modo legale e distribuisce volantini che promuovono alternative ecologiste allo status quo attuale, ad esempio la dieta vegana, la richiesta di finanziamenti per le piste ciclabili e un minor utilizzo dell'auto personale. Usano una mailing list su un server radicale fidato.

Premesse

Il collettivo presume che la polizia tenga genericamente sott'occhio gli attivisti, ma di non essere oggetto di particolare attenzione. Sanno che ai troll piace molestare i "fricchettoni". Sanno anche che ci sono organizzazioni ecologiste più militanti nella loro regione, e che le persone del proprio collettivo partecipano anche ad altri gruppi.

Contromisure

Il collettivo vuole evitare le molestie, quindi tiene la mailing list privata e su invito. Vogliono evitare tracciamenti dai grandi provider di email, quindi ne usano uno proprio.

Analisi

Le mailing list sono molto usate perchè chiunque ha accesso alla mail, mentre ci sono molte app di messaggistica e non tutti usano le stesse. Spesso le persone dicono di non avere memoria sul telefono per nuove app. Alcuni membri del collettivo non hanno grandi capacità tecniche e non vogliono imparare ad usare nuove app, quindi a volte è inevitabile usare la mail. Gli ecologisti di tutto il mondo, anche nelle cosiddette democrazie occidentali, sono sotto particolare sorveglianza anche se non propensi all'azione diretta. Una mail su un provider privato può abbassare il rischio di intercettazioni, ma c'è sempre qualche anello debole in caso di richiesta dei dati dalle autorità giudiziarie. Un grosso provider può ottemperare alla richiesta senza avvisare il collettivo, e anche se i server radicali che gestiscono il server per il collettivo lo farebbero sapere al collettivo senza problemi nonostante un obbligo a tacere, la polizia potrebbe aggirarli chiedendo direttamente alla compagnia che ospita il server di avere quei dati. In più i server radicali devono essere competenti e affidabili poichè è possibile che piccoli gruppi potrebbero non avere le competenze tecniche dei grandi provider di email per tenere sicuro il server o far sapere se viene violato dai troll di Stato.

Consigli

Se il problema è lo spazio sul telefono, le persone dovrebbero fare un backup di foto e video e cancellarle tutto sul telefono per fare spazio. Questa è in generale una buona pratica per salvare dati in caso si perda o rompa il telefono. Il collettivo dovrebbe spostare le comunicazoni su un'app di messaggistica con crittografia, ma se continuano a usare le email, dovrebbe essere solo per i dettagli più semplici come luogo e ora delle loro attività. Organizzazione, dibattito interno, discussioni

Reti Cellulari

Le reti cellulari prendono il loro nome dalla sovrapposizione di molteplici celle fornite dalle torri telefoniche che ricevono e trasmettono il segnale.[3] Nelle aree urbane c'è una copertura molto fitta, per cui un singolo telefono è in contatto con più torri. Nelle aree suburbane e rurali, c'è meno sovrapposizione, di conseguenza un telefono è in contatto con poche torri.

Gli operatori di rete possono usare informazioni sul segnale inviato al telefono per stimare la posizione dei dispositivi riceventi. La posizione approssimativa può essere determinata dall'angolo di arrivo alla torre oppure sapendo da quale settore[4] arriva il segnale. Quando la distanza di un telefono è misurata simultaneamente da più torri, il fornitore di rete può triangolare la localizzazione in modo molto accurato.[5] Le reti LTE (4G) possono identificare la posizione entro una decina di metri, mentre le 5G hanno una precisione di 5 metri. Più torri ci sono, più la posizione può essere determinata con accuratezza; di conseguenza, le triangolazioni rurali sono solitamente meno esatte di quelle urbane.

Quando i telefoni si connettono a una rete cellulare mandano un codice identificativo del dispositivo (IMEI[6]), insieme al loro codice di sottoscrizione (IMSI[7]). Un codice IMSI è normalmente memorizzato su una SIM fisica[8] o su una eSIM[9]. Ciò significa che scambiare diverse SIM card in un dispositivo oppure sostituire una SIM card con più dispositivi può creare un collegamento fisico evidente tra la vecchia SIM e la nuova SIM con lo stesso telefono. Per effettuare delle chiamate, non sono richiesti una SIM o un IMSI validi, questi sono richiesti solo perchè è necessaria un autenticazione del dispositivo collegato al carrier ovvero al gestore telefonico che è in grado di determinare se il dispositivo ha il permesso di fare telefonate o usare i dati mobili. Per esempio, le chiamate d'emergenza possono essere fatte anche senza SIM. Rimuovere la scheda dal proprio telefono, non previene dall'essere tracciato con il codice identificativo del dispositivo.

Tipologie di telefoni

La maggior parte delle persone usa il termine "telefono" riferendosi allo "smartphone", vale a dire quello con un sistema operativo e varie applicazioni che possono essere installate direttamente da chi lo utilizza. I semplici telefoni (SIMPLE PHONE) invece sono quelli meno sofisticati tra tutti i tipi esistenti, di quelli visti sin dai primi giorni della diffusione dei cellulari: effettuano solo chiamate e inviano sms. Piuttosto rari al giorno d'oggi i Feature Phones. I feature phones sono più o meno una via di mezzo tra lo smartphone e un simple phone. Potrebbero avere app

[3] non tutte le celle sono torri, ma è sufficente usare il termine generico

[4] L'area a forma di cono coperta da una singola antenna.

[5] Questo processo viene chiamato "uplink multilateration". Da notare che noi usiamo il termine "triangolazione" per indicare "multilaterazione" perché in questo caso abbia senso semplificare un termine per una migliorene la comprensione del processo di localizzazione.

[6] International Mobile Equipment Identity

[7] International Mobile Subscriber Identity

[8] SIM: Subscriber Identity Module

[9] una scheda SIM integrata, un chip integrato direttamente nel dispositivo

specifiche del produttore (VENDOR) come ad esempio, un programma per le email o un browser integrato per andare su internet. Per distinguere i feature phones e i basic phones dai più comuni smartphone, useremo il termine "simple phone" per entrambe le tipologie.[10]

Smartphone

Una delle funzionalità degli smartphone è il servizio di geolocalizzazione che permette al telefono di fornire informazioni sulla posizione in tempo reale alle varie applicazioni, prima fra tutte maps. Il servizio di localizzazione usa segnali ricevuti dai satelliti GPS[11] o GLONASS[12] per triangolare la posizione del telefono. La maggior parte dei cellulari usa il GPS assistito (A-GPS)[13] che combina i segnali ricevuti dalle torri cellulari, dal WI-FI, ma anche dallo scambio di dati su internet per calcolare velocemente e con maggiore precisione la posizione.

Gli smartphone spesso sono dotati anche di una bussola, un accelerometro, un giroscopio e un barometro. Anche senza GPS o multilaterazione, le rilevazioni provenienti da questi sensori possono essere combinate per ottenere la posizione reale utilizzando localizzazioni precedentemente acquisite. Ciò significa che, nonostante i segnali GPS vengono ricevuti passivamente da un dispositivo, l'utilizzo dei servizi di localizzazione può trasmettere la posizione del telefono.

Inoltre, disattivare la geolocalizzazione potrebbe non essere sufficiente ad evitare che un'app o un malware sul tuo telefono siano in grado di determinare la tua posizione.

Telefoni Semplici

Molte persone che fanno attivismo credono che usare telefoni non-smartphone sia più sicuro. In realtà, questa tipologia di telefono può comunque essere geolocalizzata sebbene non abbia il GPS o il servizio di localizzazione; di conseguenza, non offre una protezione significativa nel rilevamento della posizione. Nei feature phone, in genere, non sono presenti applicazioni di chat vocali o di testo: i telefoni semplice non-smartphone, per definizione, non hanno queste funzionalità. Ciò significa che si possono solamente effettuare telefonate e mandare sms non codificati; tuttavia sono vulnerabili alle intercettazioni in più modi di quelli che possono andare su internet e possono cifrare i messaggi. I telefoni non-smartphone, apparentemente i meno avanzati tecnologicamente, arrivano al massimo ad usare il 2G; ciò vuol dire che con appena 25€ di attrezzatura tecnica le telefonate e gli SMS sono facilmente intercettabili. Inoltre, molti di questi dispositivi posseggono "funzionalità internet" nascoste che inviano i dati telemetrici ai produttori senza che chi li utilizza ne sia consapevole.

[10] Alcune persone utilizzano il termine "dumb phone" per i due tipi di telefoni semplici; stiamo evitando appositamente questa espressione per fare chiarezza.

[11] Sistema di posizionamento globale, gestito dal dipartimento della difesa statunitense.

[12] Sistema globale di navigazione satellitare, un GPS alternativo gestito dall' agenzia spaziale russa Roscosmos.

[13] GPS assistito

Consigli

Visto che prevedono una sorveglianza mirata sulle loro attività, dovrebbero lasciare tutti i dispositivi elettronici a casa e scegliere per i loro incontri posti casuali, che siano molto isolati o molto rumorosi.

Caso 6: Telefoni e manifestazioni di massa

Scenario

Isa è un'attivista che partecipa alle grandi manifestazioni e anche se lei non è particolarmente radicale ha degli amici che lo sono, e di solito è al corrente di quel che fanno. I fascisti hanno organizzato una marcia e Isa e alcuni amici si uniranno al gruppo che spera di bloccare il percorso che i fascisti vogliono fare. Per stare in contatto con gli amici ed essere aggiornata sui blocchi o i cambi di percorso, Isa porta con sè il telefono che usa di solito (che è anche l'unico).

Premesse

Isa non teme l'arresto perchè in situazioni del genere in passato, cioè quando una grande massa di gente blocca le strade, di solito la polizia cerca di arginarla o portarla lontano prima di far passare i fascisti. Non pensa che se fosse mai arrestata guarderebbero il suo telefono, in modo legale o illegale. Non si preoccupa nemmeno della sua localizzazione.

Contromisure

Isa non prende contromisure per non far raccogliere dati sulla sua posizione o per non farsi sequestrare il telefono.

Analisi

Nelle manifestazioni di massa la polizia può usare IMSI-catcher per vedere chi ha partecipato e tracciarne i profili. In questi casi la posizione può essere usata per perseguire delle persone per eventuali scontri, anche se magari la denuncia non si tramuta in condanna. Se Isa viene arrestata, cosa che comunque può succedere se i blocchi sono piccoli o se è tra le sfortunate che vengono acchiappate mentre si formano i blocchi, il suo telefono potrebbe essere ispezionato. Da questo la polizia può scoprire i suoi legami e le attività dei suoi amici più radicali. In sostanza questo può mettere in pericolo loro più che lei.

Consigli

Anche se Isa non mette in conto l'arresto, dovrebbe essere più attenta col telefono. Può mettersi d'accordo con gli amici di incontrarsi in un certo punto prima della manifestazione così può non portarsi dietro il telefono, o se proprio vogliono avere informazioni in tempo reale, solo una persona del gruppo dovrebbe portarsi il telefono. Prestare attenzione al suo telefono può proteggere i suoi amici che partecipano ad azioni più rischiose. Comunque, le probabilità che succeda una di queste cose è bassa, mentre è molto utile che lei si porti il telefono. Questo lo rende un caso in cui "ci sta" che Isa si porti dietro il telefono… finchè non va male.

Consigli

Ruben dovrebbe usare uno smartphone per le comunicazioni in generale. Se a volte ha bisogno di nascondere dove si trova o non farsi intercettare, deve lasciare il telefono a casa.

Caso 5: organizzarsi senza telefono

Scenario

I membri di un gruppo di affinità fanno parte dei movimenti da tempo e sono ben conosciuti dallo Stato. Stanno preparando qualcosa di grosso. Non ne parlano tramite dispositivi elettronici, ma solo di persona.

Premesse

Danno per scontato che lo Stato farà di tutto per prevenire la loro azione e soprattutto dopo per investigare. Pensano sia possibile che ci siano dei malware dello Stato sui loro dispositivi. Pensano che anche senza prove, saranno proprio loro i primi della lista dei sospetti per questa azione, quindi il loro livello di sicurezza deve essere impenetrabile.

Contromisure

Vista la possibilità dei malware, ritengono i loro dispositivi non affidabili. Vista la probabilità di essere oggetto di indagine, non parlano dell'azione a casa, in auto, negli spazi di movimento e in quelli dove bazzicano di solito. Per ridurre i metadati delle comunicazioni tra loro, spengono i telefoni prima di arrivare al luogo di incontro e li riaccendono solo dopo essersene andate.

Analisi

Il gruppo fa bene a pensare di essere sotto sorveglianza e fa bene a trattare i telefoni come spie. Spegnere i telefoni diminuisce la possibilità di essere ascoltati da malware che si servono dei microfoni, e serve anche in una certa misura a nascondere la loro posizione durante gli incontri. Ma l'assenza di queste informazioni può essere strana se confrontata con quella del loro utilizzo normale dei telefoni, e il fatto che tutti i loro telefoni spariscano contemporaneamenti nei pressi di uno stesso posto può essere un indizio per lo Stato. Questo può essere motivo di ulteriore sorveglianza e portare, ad esempio all'istallazione di cimici in quel preciso posto—se usato più volte—o mandare uno sbirro in borghese nel bar dove si trovano. In più, se un membro del gruppo viene arrestato e non dice niente negli interrogatori, comunque la polizia può guardare il suo telefono in cerca di anomalie. Ad esempio: all'ora in cui questo telefono è stato spento, quali altri telefoni sono stati spenti nelle vicinanze? E cosa facevano i telefoni degli altri sulla lista dei sospetti? Questo può rivelare il resto del gruppo di affinità o dare elementi per provare che proprio quelle persone erano le complici. È possibile che la polizia non faccia queste operazioni, ma è meglio non lasciare traccia.

In sintesi, facendo riferimento alla maggior parte delle minacce che ogni attivista si trova ad affrontare, possiamo concludere che i cellulari **non-smartphone non sono molto più sicuri degli stessi smartphone**.

Malware

Un malware è un software dannoso, come un virus. E' un app sul tuo telefono che fa qualcosa che tu non vuoi e cerca di essere invisibile. I malware creati dallo stato, spesso, hanno soltanto il fine di sorvegliare e diffondersi su altri telefoni o persino ad su altri dispositivi elettronici, come il tuo computer o il router wifi di casa.

Diversi siti di prevenzione e sicurezza digitale ci informano che un malware nella maggior parte dei casi viene installato visitando siti web non sicuri o aprendo allegati su email da mittenti sconosciuti; sebbene tutto ciò sia vero, sappi che l'area di attacco del tuo telefono è molto più vasta. La maggior parte delle app ricevono e inviano messaggi che arrivano da servizi intermediari come Google Play per poi inviare le richieste ai reali server delle applicazioni come Whatsapp. Alcuni malware hanno un sistema detto "zero-click", vale a dire che non necessitano di alcuna interazione. Un esempio è lo spyware Pegasus della NSO (azienda israeliana attiva nel settore informatico, nota proprio per aver inventato Pegasus che consente di sorvegliare da remoto gli smartphone) che ha usato un exploit zero-click e ha preso di mira chi fa attivismo, chi fa giornalismo e varia fauna politica mondiale.

I malware possono essere installati sul tuo telefono anche se usi solo applicazioni sicure e accetti messaggi da contatti affidabili. Altri tipi di malware, invece, stanno nella memoria del tuo telefono mentre è acceso e scompaiono dopo un riavvio. Per questo motivo, alcuni malware fingono la routine di spegnimento del telefono per poi eseguire uno spegnimento falso. Tuttavia, considera che il riavvio e il reset periodico del tuo telefono può potenzialmente eliminare un malware.

Se pensi che il tuo telefono sia stato compromesso, avrai bisogno di una persona specialista di malware, una persona che sia in grado di scoprirlo e, probabilmente, considera che dovrai procurarti un nuovo cellulare. I malware sono meno comuni di quanto pensi, ma non far sì che questa informazione ti porti ad ignorare legittimi segnali di avvertimento. Quelli sponsorizzati dallo stato non saranno facilmente individuabili come gli altri tipi (low-effort malware), dunque i metodi comuni potrebbero non essere applicabili. Sfortunatamente, non è possibile rilevare questi software dannosi in autonomia.

Sistemi operativi

"Qual è il più sicuro, iOS o Android?" Questa è una delle domande più comuni che ogni attivista si pone sugli smartphone.

E, come in tutte le domande sulla sicurezza, la risposta è "Dipende". I sistemi operativi degli smartphone si dividono in due tipologie: iOS per dispositivi Apple e Android per tutti gli altri. iOS è brevettato con un codice sorgente privato. Android è un sistema operativo di base con codice di sorgente pubblica che i produttori possono modificare per i loro dispositivi. I produttori dei sistemi operativi Android, di solito, hanno un codice sorgente privato. Inoltre, ci sono diverse versioni integrali

per Android gestite dalla comunità open source, la più nota è LineageOS [14]. GrapheneOS and CalyxOS sono sistemi operativi Android open source personalizzati e modificati per avere una notevole attenzione alla privacy e alla sicurezza.

Quando un cellulare è acceso, l'hardware inizia a caricare il sistema operativo usando un processo in cui ogni fase verifica l'integrità del software necessario per il passaggio successivo. Questo procedimento è definito in diversi modi come, ad esempio, secure boot or verified boot (avvio sicuro o avvio verificato). Per installare un sistema operativo personalizzato, il processo di avvio verificato deve essere disattivato, altrimenti l'hardware rifiuta di caricare il sistema operativo poichè non è crittograficamente firmato da una chiave sicura, la quale era già inclusa dal produttore originale. Questo comporta che un sistema operativo dannoso, installato al posto di quello autentico, possa leggere i tuoi dati mediante un accesso fisico o un malware. Tuttavia, ciò non significa che un sistema operativo standard sia più o meno sicuro di uno personalizzato, ma vuol dire che c'è un profilo di rischio diverso quando si disattiva l'avvio sicuro e si utilizza un sistema operativo personalizzato.

Quando il malware viene sviluppato, prende di mira una singola applicazione o il singolo sistema operativo. Lo sviluppo di malware è molto dispendioso in termini di tempo e denaro; in più, una volta sviluppato può essere rilevato e reso incapace di infettare nuovi dispositivi tramite aggiornamenti dell'app presa di mira [15]. Di conseguenza, è più economico creare malware che possono colpire più utenti. iOS ha un numero limitato di versioni per un numero limitato di dispositivi, mentre l'ecosistema Android è variegato e parecchio diverso. Pertanto, per un avversario è meno economico e più difficile colpire tutti i fruitori di Android.

Di seguito le nostre raccomandazioni:

- Per la maggior parte delle persone che provano ad evitare la sorveglianza di massa e gli hacker della domenica/di basso profilo, sono sufficienti sia iOS sia un sistema operativo Android standard, in quanto più facili da usare.
- Per le persone che sono coinvolte in maniera significativa nei movimenti sociali o che credono di essere prese di mira singolarmente, attualmente raccomandiamo per il loro lavoro organizzativo e politico di usare un sistema operativo Graphene senza Google Play, di usare f-droid come unico archivio di app e installare solo un numero minimo di applicazioni richieste per le comunicazioni.
- Per le persone che hanno attirato o pensano di attirare l'attenzione degli apparati investigativi, i telefoni dovrebbero essere evitati per tutto ciò che riguarda l'attivismo.

[14] LineageOS è il successore del popolare CyanogenMod il cui sviluppo è stato sospeso nel 2016.

[15] In aggiunta, un malware ha un'interessante caratteristica: quando viene utilizzato può essere copiato e clonato in modo che anche altri possano riusarlo. E' come se ogni volta che viene lanciato un missile in territorio nemico, ci fosse la possibilità di copiarlo all'istante e riprodurlo all'infinito e che quel modello di missile possa essere intercettato e bloccato anche nel futuro. I militari sarebbero più titubanti nel lanciare così tanti missili, farebbero attenzione e avrebbero bisogno di essere più strategici nei confronti dei loro obiettivi.

Ma occhio al telefono "pulito". Visto che alcuni del gruppo rimangono fuori a volto scoperto, l'identità del gruppo è in generale riconoscibile, anche se non si può sapere con esattezza chi è dentro l'edificio. Se il telefono pulito è di qualcuno o è stato acceso a casa di qualcuno, questa può essere usata come prova che quella persona si trovava all'interno dell'edificio.[24] Attenzione anche al fatto che la polizia può usare un ricevitore di IMSI-catcher per leggere gli SMS in tempo reale e agire in base alle comunicazioni.

Consigli

Il motivo per cui il gruppo di occupazione vuole portarsi solo un telefono è legittimo, ma devono usare un telefono con un account usa e getta usando Signal. Questo account deve comunicare solo con un altro account anonimo per evitare di dare informazioni in caso venga confiscato.

Caso 4: telefono semplice + Signal su computer

Scenario

Ruben è militante in un gruppo di persone che credono sia sotto sorveglianza per le loro istanze antigovernative. Per minimizzare le possibilità che la polizia lo localizzi, usa un telefono semplice con SIM quando è in giro. Visto che alcuni discorsi con il suo gruppo sono più sensibili hanno bisogno di un sistema di messaggistica più sicuro e hanno scelto Signal. Signal richiede di registrare un numero di telefono e genera la crittografia iniziale solo sulle app iOS o Android. Per far funzionare Signal su PC ha usato la SIM card del suo telefono nello smartphone di un amico per impostare una coppia di codici iniziali da collegare al suo PC. Dopo, Ruben fa logout sul telefono dell'amico e cancella Signal.

Premesse

La scelta di Ruben di non portarsi dietro uno smartphone si basa sulla convinzione che gli smartphone siano più facilmente tracciabili dei telefoni normali. Ruben presuppone anche che Signal sia più sicuro delle chiamate o degli SMS.

Contromisure

La scelta di Ruben di usare un telefono semplice ha l'obiettivo di diminuire le possibilità di tracciamento. La scelta di Signal è per evitare le intercettazione dei messaggi con altre persone.

Analisi

La posizione di Ruben è tracciabile praticamente nella stessa maniera con un telefono semplice e con uno smartphone. Le sue comunicazioni sono meno sicure perchè col telefono semplice non ha la possibilità di mandare o ricevere messaggi "di emergenza" con le persone di fiducia, e se lo fa, i suoi contatti saranno intercettati.

[24] *ndt*: questo vale anche in casi diversi dall'occupazione.

chi si organizzava prima ha visto il cambiamento per cui pian piano ognuno aveva sempre un microfono con sé.

Come detto sopra, gli smartphone ci permettono di comunicare in modo istantaneo e avere informazioni illimitate a portata di mano, in ogni momento. Tutto ciò a prezzo di nuove tecniche di sorveglianza. Bisogna essere consapevoli che i telefoni in casa, in macchina e negli spazi sociali possono raccogliere informazioni di contorno sui gruppi. Se consigliassimo di spegnere più spesso i telefoni, saremmo persone paranoiche o direbbero che è infattibile. La cosiddetta democrazia liberale dà l'illusione che non viviamo in uno stato di polizia, eppure ci sono molti casi di gruppi innocui che vengono sorvegliati, per non parlare di quelli più radicali e attivi.

Non diciamo che non dovremmo mai avere il telefono dietro, ma vogliamo che tutti e tutte siano più consapevoli dell'impegno dello Stato nella sorveglianza e dell'utilità delle informazioni raccimolate da conversazioni qualunque. Forse verrà il momento in cui la repressione si inasprirà e cominceremo a sentire di più la sua presenza. Per prepararci a quei tempi e abituarci a resistere, il nostro consiglio è più moderato: alzare il livello di sicurezza ora. Provate a organizzare eventi senza telefoni. Quando vi fate i fatti vostri, andate a camminare in montagna, anche se vi vedete al pub, provate a fare in modo che ognuno lasci i telefoni a casa. Abituatevi alla loro assenza. Provate l'ebbrezza di non regalare dati allo Stato e sapere che solo i presenti possono sentire le vostre conversazioni.

Caso 3: le occupazioni e i telefoni semplici

Scenario

Un gruppo di persone vuole occupare un edificio abbandonato per attirare l'attenzione sulla speculazione edilizia e farlo diventare una casa per gli abitanti della zona che sono stati appena sfrattati. Un gruppetto entra nel posto mentre gli altri stanno fuori e postano sui social.

Premesse

Il gruppo di occupazione pensa che la polizia possa capire la loro identità guardando che telefoni stanno comunicando da dentro l'edificio, e anche se non verranno arrestati o perseguitate stavolta, questa informazione potrà essere usata contro di loro in futuro.

Contromisure

Per ridurre il rischio di svelare la loro identità, il gruppo di occupazione ha scelto di non portare i telefoni personali. Porteranno solo un telefono "pulito" per comunicare con il gruppo fuori e per evitare di rimanere isolati fino alla fine dell'azione. Useranno una SIM senza nominativo per mantenere completo anonimato.

Analisi

Il gruppo fa bene a non portarsi il telefono durante l'occupazione. La polizia potrebbe scoprire le loro identità guardando quali telefoni si trovano dentro all'edificio.

Crittografia dei dispositivi

iOS e Android offrono la possibilità di crittografare i tuoi dati personali, sotto il nome di Sicurezza e Crittografia del telefono. In genere, solo i telefoni più recenti hanno la crittografia del dispositivo di default. Questa funzione però può essere abilitata dall'utente sia durante la configurazione del telefono che in un secondo momento. Inoltre è consigliabile abilitare la protezione contro eccessivi tentativi di login sul proprio telefono.

L'attuazione della crittografia dei dispositivi usa solitamente un HSM, ovvero un modulo di sicurezza hardware, sono chip speciali nel telefono che gestiscono i dati crittografati all'interno del telefono[16]. Questi chip sono importanti poichè proteggono le chiavi da accessi non autorizzati o manomissioni sul tuo telefono; possono impedire alla controparte di accedere ai tuoi dati, se tu non hai dato la tua password, ma non è assicurato che funzioni sempre. Esiste ad esempio uno strumento chiamato Grey-Key che è in grado di sfruttare i bug dentro dei chip HMS e, in alcuni casi, è stato in grado di decifrare la password di sblocco ed avere quindi accesso ai dati. Gli HSM che oggi sono sicuri potrebbero avere nuovi bug il mese successivo; la polizia potrebbe sviluppare nuove tecniche per recuperare i dati nei prossimi 5 o 10 anni. La crittografia del dispositivo fa un buon lavoro impedendo accessi ai tuoi dati nel caso in cui uno spione ottiene l'accesso fisico al tuo telefono o se uno sbirro te lo sequestra durante una perquisizione. E' improbabile resistere ai tentativi combinati di accesso ai tuoi dati da parte degli apparati investigativi.

Un esempio di grande risonanza è stato quando l'FBI ha decifrato la password del telefono dell'omicida di massa ad un anno dalla sparatoria di San Bernardino del 2015. Dopo 5 anni dall'accaduto, è stato rivelato che l'accesso ai dati era stato fatto tramite usando dei bug che esistevano nell'HSM.

In generale l'uso della crittografia potrebbe aiutare a poteggersi dall'acquisizione dei dati, ma **l'unico modo per assicurarsi che non finiscano nelle mani sbagliate è far sì che non siano mai esistiti.**

VPN

Una rete privata virtuale (VPN) si riferisce a un' applicazione che indirizza il traffico internet di un dispositivo a un servizio esterno il cui scopo è solo quello di nascondere il traffico web dell'utente usando un altro indirizzo di rete. Rendendo molto pià complicato identificare chi sta navigando o controllando le email, la VPN protegge le tue attività sul web nascondendo il tuo indirizzo di rete (IP address). Quando usata, la VPN permette di nascondere il proprio indirizzo dietro reti wifi pubbliche permettendo di connettersi e navigare di forma più sicura. Inoltre, può sviare le indagini e rendere la sorveglianza passiva più difficile, ma potrebbe anche succedere che possa avere dei malfunzionamenti di per se o semplicemente ti dimentichi di attivarlo e facendo così potresti creare un esposizione del tuo indirizzo reale permettendo a chi vuole di identificarti. Il traffico da e verso il tuo provider VPN può essere collegato agli apparati monitorati dello stato che sono in grado di

[16] Sui dispositivi Apple questo chip si chiama Secure Enclave.

osservare tutto il traffico internet e, di conseguenza, ogni servizio di VPN è legalmente costretto ad acquisire e cedere i registri delle tuo traffico (logs) alle forze dell'ordine. Le VPN sono economiche, possono incrementare la sicurezza in vari modi, ma sarebbe meglio non farci affidamento per garantire l'anonimato contro lo stato.

IMSI Catchers

Un ricevitore IMSI[17] è un dispositivo che si comporta come un normale ripetitore telefonico e induce i telefoni vicini a connettersi ad esso, permettendo così l'intercettazione o l'invio di SMS o chiamate. A volte, la manomissione (spoofing) è rilevabile, ma non sempre è facile individuarli. In alcune regioni, questi ricevitori possono essere impiegati senza mandato, soprattutto durante le manifestazioni. In parte, lavorano diminuendo il protocollo ad uno senza crittografia o con una crittografia fragile così da poter intercettare la conversazione. Sebbene gli smartphone abbiano impostazioni per protocolli che offrono una maggiore protezione contro intercettazioni e manomissioni, è possibile far sì che i telefoni funzionino anche solo con il 2G che fa parte del GSM standard, è quindi possibile essere declassati per usare i protocolli non sicuri dei ricevitori IMSI. Usando questa tecnica le telefonate e i messaggi inviati e ricevuti dagli smartphone non resistono alle intercettazioni dei ricevitori IMSI.

Borse di Faraday

I telefoni mandano e ricevono informazioni usando radiazioni elettromagnetiche, le quali possono essere bloccate da materiali speciali. Leggende metropolitane e alcuni elementi di prova affermano che i segnali possono essere bloccati mettendo il telefono in uno o più sacchetti di patatine[18], i quali hanno una pellicola interna, ma questa, così come molte altre contromisure, non dovrebbe essere presa seriamente in considerazione. Può essere aquistato o costruita una gabbia o borsa di Faraday e farci affidamento per bloccare i segnali telefonici.

Se hai bisogno di portarti dietro il telefono ma vuoi avere la sicurezza che non trapeli nessun tipo di segnale, allora spegnerlo potrebbe non essere sufficiente. Sono pochi gli smartphone a cui è possibile rimuovere la batteria. Qualcosa che poggia sul telefono nella tua borsa potrebbe premere il bottone di accensione. I malware possono fingere lo spegnimento e impedire al telefono di spegnersi realmente mentre stai provando a farlo. Mettere telefoni spenti in una borsa di Faraday può evitare che il telefono mandi segnali ed evitare considerevolmente la possibilità di stabilire il tuo segnalo o la tua posizione.

Le basi della sicurezza

Ci sono alcune pratiche legate all'uso dei cellulari che sono consigliabili per la maggior parte delle persone che vogliono fare attivismo. Alcune di queste consigli

[17] Spesso i ricevitori IMSI vengono chiamati StingRay, nome di una nota azienda di ricevitori

[18] anche conosciute come buste di alluminio o buste delle patatine dagli yankee.

un reato, meglio se lasciano i telefoni a casa o li spengono prima di spostarsi verso il luogo della riunione. Ancor meglio non portarsi gli stessi telefoni durante l'azione. Se si vuole un alto livello di sicurezza, la sorveglianza del luogo e dei telefoni si può ridurre ancora ritrovandosi fuori dagli spazi di movimento. Se invece per convenienza il gruppo vuole trovarsi in un luogo centrale e conosciuto, all'inizio dell'assemblea bisognerebbe stabilire di parlare solo dell'azione in questione e non di alte cose illegali.

Caso 2: Chiacchiere spiate

Scenario

Alcune persone appartenenti a un gruppo di affinità sono in un parco a farsi i fatti loro senza organizzare niente. Hanno i telefoni accesi ma per sicurezza hanno l'abitudine di non parlare di azioni passate o scambiarsi storie visto che possono contenere indizi incriminanti.

Premesse

Questo gruppo dà per assodato che la polizia voglia solo ascoltare le loro conversazioni se riguardano attività illegali passate o future, mentre le loro discussioni quotidiane non sono interessanti.

Contromisure

Il gruppo non prende nessuna contromisura per evitare che le chiacchiere siano spiate.

Analisi

Se intenzionalmente nessuno parla di piani o azioni, ovviamente nessun microfono potrà mai sentire ciò che non viene detto. Però le azioni non sono l'unica cosa per cui lo Stato ha interesse. Gossip, drammi, fatti amorosi, legami e anche la propensione reciproca di persone o organizzazioni all'interno di un movimento sono un elemento di interesse. Tutto questo aiuta lo Stato a farsi una mappatura sociale dettagliata. Se lo Stato sospetta che un individuo fosse coinvolto in qualcosa su cui sta indagando e sa che quella persona aveva dei complici, usare queste mappe costruite su pezzi di conversazioni casuali può aiutare ad accorciare le fila dei sospetti o rivelare i membri di un gruppo di affinità. Spiare le chiacchiere può rivelare allo Stato chi si sente escluso o risentito per tentare di farlo diventare un informatore. Può sfruttare piccoli conflitti o soffiare sull'emotività per fomentare conflitti interni.

Consigli

C'è un gap generazionale tra chi si organizzava già prima della diffusione dei cellulari e chi ha iniziato dopo la loro proliferazione. C'è anche un altro gap tra chi si organizzava con i telefoni prima della diffusione degli smartphone e chi si orgaizza da sempre in un mondo in cui quasi tutti i loro contatti hanno uno smartphone. Questo gap si nota dalla capacità di organizzarsi senza telefoni, ad esempio fissare luogo e ora di un appuntamento senza cambiamenti dell'ultimo minuto. In più,

sono dei ripieghi e il tuo piano deve prevedere che questi metodi possano a un certo punto essere gli unici validi per comunicare.

Casi di studio

Per rendere ciò che abbiamo discusso più concreto vi riportiamo qualche caso studio preso dalla nostra esperienza. In alcuni di questi casi ci sono individui che hanno già un threat model dettagliato e alcuni che non ce l'hanno. Alcuni sono basati su leggende metropolitane e altri su fatti verificabili o congetture verosimili. Laddove ci sono degli errori sono analizzati.

Caso 1: pianificare assemblee per un'azione semi-pubblica

Scenario

Un collettivo sta preparando un'occupazione che deve rimanere segreta fino al momento in cui avviene, dopodiché sarà pubblicata sui social. Si prepara per la maggior parte in assemblee di persona in uno spazio sociale.

Premesse

Il collettivo dà per scontato che la polizia sia interessata a prevenire le occupazioni e che ogni persona possa essere sorvegliata. Questa sorveglianza include, ma non si limita a, malware che lo Stato può mettere sul telefono di ogni persona.

Contromisure

Per impedire allo Stato di usare il microfono dei telefoni per registrare le riunione, tutti i telefoni vengono messi in una scatola di plastica sigillata in un'altra stanza.

Analisi

E' vero che i telefoni possono essere compromessi da malware ed è vero che metterli in un'altra stanza impedisce che i microfoni registrino una conversazione. Però c'è un presupposto necessario per l'efficacia di mettere i telefoni in un'altra stanza, che può essere verificato iniziando a registrare con un telefono, metterlo nella scatola e iniziare una conversazione ad alta voce per vedere quanto si sente. Se le voci sono anche lontanamente riconoscibili, i frammenti della conversazione si possono recuperare con un software di editing audio. Se lo spazio non viene ripulito regolarmente da microfoni e altre cimici, la conversazione potrebbe comunque essere registrata. Se il gruppo o altri che frequentano il posto sono sorvegliati da vicino, potrebbero esserci dei microfoni direzionali che registrano le conversazioni dagli edifici vicini. Se alcuni individui sono sottoposti a sorveglianza passiva (metadati), la presenza ripetuta dello stesso gruppo di telefoni nello stesso posto dalle 19 alle 21 per qualche mercoledì di seguito può svelare che c'è stata una riunione e quali erano i partecipanti.

Consigli

Se si tolgono i telefoni è meglio spegnerli anche. Meglio se vengono messi in un posto rumoroso per minimizzare le possibilità che carpiscano i suoni della conversazione. Se il gruppo ritiene di poter essere perseguito per la sola preparazione di

e pratiche sono riportate di seguito.

Aggiornamenti

In linea generale, la prima cosa che si può fare per prevenire intrusioni da parte delle forze dell'ordine—o di hacker a caso—è installare gli aggiornamenti del sistema operativo dello smartphone e di tutte le app. Può essere una scocciatura, ma molti aggiornamenti contengono delle patch di sicurezza per vulnerabilità critiche. Se non altro, ciò può evitare che i tuoi account bancari e di pagamento vengano prosciugati.

Password Manager

La seconda pratica più utile e generalmente applicabile è usare un gestore di password (Password Manager) per tutti i tuoi account, inclusi quelli sul tuo telefono. Ce ne sono versioni a pagamento che permettono la sincronizzazione automatica delle password tra dispositivi e il login automatico alle pagine web. Tuttavia, questi richiedono un certo livello di fiducia nell'azienda che offre il prodotto. Esistono alternative gratuite come KeePassXc[19] che però non hanno la stessa facilità d'uso dei prodotti a pagamento. Quando si usa un Password Manager, tutti i tuoi account dovrebbero avere password forti, uniche e casuali, che comunemente vengono generate in automatico dal programma stesso. La password "master" per sbloccare il programma dovrebbe essere una frase lunga e casuale.

Le persone sono notoriamente pessime nel generare buone password e anche usando il verso iniziale del tuo poema preferito o qualche articolata sostituzione di caratteri per trasformare `antifascismo` in `4n7if4sc1sm0!` il che può far pensare di rendere le password difficilmente crackabili da parte dei computer, ma non è così. Il "diceware" è un metodo di creazione delle password che lancia un immaginario dado e utilizza i numeri ottenuti per selezionare delle parole all'interno di una lista predefinita. Cinque parole è il minimo assoluto, sei è meglio, mentre qualsiasi combinazione oltre le otto parole è persino esagerata. Fare questo permette di ottenre una casualità impossibile da indovinare, che non si potrebbe mai ottenere autonomamente, inoltre una frase è facilmente memorizzabile. Una lista di termini in inglese facilmente utilizzabile è fornita dall'EFF (Electronic Frontier Foundation). Una frase di esempio è CambiaCalmaBollaRestaGiusta (si prega di non utilizzarla; creane una tua).

Tabella 1: Parole di esempio dell'EFF per il "diceware"

Numeri	EFF	Italiano
`24311`	drowsily	divine
`24312`	drudge	divini
`24313`	drum	divino

[19] https://keepassxc.org

Numeri	EFF	Italiano
24314	dry	divisa
24315	dubbed	divise
24316	dubiously	divisi
24321	duchess	divora
24322	duckbill	divori

Blocca il tuo telefono

A seconda della minaccia, potresti voler rendere difficile se non addirittura impossibile sbloccare il tuo telefono. Questo perché il metodo di sblocco è anche il metodo di decrittazione, per cui un metodo di sblocco forte aiuta a difendersi da accessi indesiderati ai tuoi dati se il tuo telefono viene preso. In generale, dovresti preferire le Password ai PIN e ai tracciati di sblocco telefono, dal momento che le passowrd sono più difficili da crackare. Dovresti sicuramente anche disabilitare e non usare lo sblocco facciale e preferibilmente anche lo sblocco tramite impronta digitale. In alcune regioni vi sono protezioni giuridiche per le password, ma non per le impronte o per altri dati biometrici.

Alcuni telefoni offrono la possibilità di cancellare tutti i dati sul telefono se avvengono troppi tentativi errati di sblocco. Ha senso valutare di attivare questa funzionalità se possibile e tenere il telefono lontano da persone moleste, piccole creature curiose e animali domestici. Si consiglia anche di disabilitare le notifiche nella schermata di blocco o, perlomeno, disattivare quelle delle app di messaggistica che contengono informazioni sensibili. Se hai la crittografica abilitata sul dispositivo, i tuoi dati sono protetti molto meglio quando il telefono è spento (o è stato riavviato, ma la tua password di sblocco non è stata ancora inserita). Se hai attivato la cifratura considera che dopo aver sbloccato il telefono al riavvio, la protezione dei tuoi dati è molto minore rispetto a quando è spento.

Molti attivisti lasciano lo sblocco con impronta abilitato perché è molto più pratico rispetto a dover digitare una password da 30 o più caratteri 100 volte al giorno. Dal momento che la praticità spesso ha la meglio sul bisogno di sicurezza, ciò rappresenta un'ulteriore ragione per considerare di non tenere dati sensibili sul proprio telefono. Comunque, venendoci incontro, se hai lo sblocco con impronta attivato puoi disabilitarlo temporaneamente configurando un app che tenendo premuto il pulsante di accessione disattivi lo sblocco con impronta digitale. Puoi farlo prima di avere interazioni con le forze dell'ordine, prima di andare a dormire o prima di lasciare il tuo telefono incustodito.

Funzionalità wireless

Un altro consiglio pratico è quello di disabilitare Wi-Fi e Bluetooth quando non li stai usando. Entrambi possono essere utilizzati per identificare il tuo telefono. In più, aumentano i potenziali punti di attacco da parte di chi tenta di entrare nel tuo telefono. Sebbene i rischi di lasciarli sempre attivi sia minimo, queste pratiche

azioni che possano avere conseguenze legali. Non creare delle prove che possano essere usate contro di te o altri.

Attenzione all'area geografica

Tutto ciò che hai appena letto, così come il resto della zine, rappresenta delle linee guida. Potrebbero anche non essere adatte al tuo caso. In particolare, alcuni accorgimenti di sicurezza digitale possono lasciare delle tracce molto visibili. Se Signal è molto poco utilizzato nella tua area, il fatto che tu lo utilizzi potrebbe renderti un obiettivo più evidente. L'uso di VPN potrebbe essere illegale. L'uso di TOR potrebbe portare a una visita della polizia. La presenza di applicazioni per la comunicazione sicura sul tuo telefono potrebbero trasformare il tuo arresto in una sparizione. Prima di scaricare qualsiasi cosa, contestualizzalo con la repressione presente nella tua area per determinare se le linee guida che abbiamo fornito siano adatte alla tua sicurezza o al contrario ti mettano in pericolo.

Alternative

E' sempre più facile dire "fai questo al posto di quello" invece che "non fare questo" e quando si tenta di cambiare comportamenti e abitudini, fornire alternative aumenta le probabilità che qualcuno effettivamente abbandoni i consueti comportamenti poco sicuri. Ci sono ottime ragioni per usare dei telefoni, e la presenza di alternative può rendere più facile abbandonare i telefoni o cambiare le proprie abitudini nell'usarli.

Le difficioltà nell'eliminare completamente il telefono sono che le persone vogliono conoscere e raccogliere informazioni, scambiarsi contatti. Un blocco note e una penna possono essere sufficienti per stilare in maniera analogica i report di assemblee in cui i dispositivi elettronici non sono permessi. Questo metodo è utile anche per scambiare contatti e addirittura, portando con sé la fingerprint crittografica del proprio dispositivo, si può stabilire una futuro canale di comunicazione sicuro anche quando non si ha con sé i propri dispositivi in quel momento. Un agenda o un calendario permettono di pianificare eventi. Stampare mappe cartacee delle aree in cui fare delle azioni può essere utile a orientarsi. Ricorda solo, in caso si decida di usare carta e penna, bisogna ricordarsi di distruggere ciò che è stato scritto e stampato dopo averlo usato.

Casi in cui il telefono è inutilizzabile

Oltre a essere utile nel presente, il tuo piano deve anche essere orientato al futuro. Nel caso in cui, a conoscenza dei rischi, tu abbia deciso di basarti sull'uso del telefono per l'organizzazione, devi considerare che in momenti di particolare repressione o in caso di catastrofi naturali Internet o i telefoni possano essere inutilizzabili. È comune che in caso di aumento della repressione lo Stato metta fuori uso le linee telefoniche o Internet per intere aree geografiche. Se la capacità di organizzazione e sicurezza si basa sul fatto che ogni persona abbia il telefono collegato a Internet, bisogna comprendere che ci si sta esponendo a dei casi in cui questo metodo può fallire. Il passaparola e il cossiddetto "sneakernet" (corrieri che trasportano dati)

cue può evitare che i sistemi automatizzati allertino le autorità. Usare soluzioni di questo tipo può permettere di ridurre gradualmente da alti livelli di sicurezza e livelli più bassi senza esporsi completamente alla sorveglianza e alla repressione di Stato. Questi metodi richiedono grande attenzione, ma sono possibili.

La preparazione di un piano

Non possiamo fingere di conoscere il tuo specifico modello di minaccia, né di poter tener conto di tutte le sfumature possibili per ogni situazione o regione geografica. Quello che possiamo fare è fornire alcune linee guida che sono applicabili in generale. Nel leggerle, devi valutare tu cosa sia applicabile al tuo caso. Cosa puoi fare nella pratica? Cosa faranno le persone degli ambienti che frequenti? Il tuo nuovo piano non deve necessariamente essere perfetto, ma deve essere migliore delle tue pratiche attuali. Può capitare che sia necessario raggiungere dei compromessi su alcuni aspetti della sicurezza al fine di poter continuare ad organizzarsi. Al tempo stesso, non lasciare che le pratiche poco sicure altrui possano metterti in pericolo. Trova il giusto equilibrio.

Questa non è in alcun modo una lista esaustiva, piuttosto alcuni metodi per sviluppare una Sicurezza Operativa per sè e migliorare la cultura della sicurezza di gruppo:

- Usa uno smart phone: sono più sicuri rispetto ai semplici telefoni per quanto riguarda la maggior parte delle minacce che gli attivisti devono affrontare.
- Non portare con te il telefono quando partecipi in attività che possano interessare la polizia, in particolare in manifestazioni che possano essere turbolente.
- Scegli applicazioni di messaggistica con crittografia End-To-End (E2EE), abilita l'cancellazione dei messaggi automatica, evita le email.
- Cifra la memoria del tuo dispositivo e imposta una password di sblocco.
- Disabilita l'accesso biometrico (impronta digitale) quando lasci il dispositivo incustodito.
- Fai dei backup regolari delle foto e altri dati su un disco cifrato; poi cancellali dal telefono.
- Cancella i dati vecchi: messaggi, chat di gruppo, email, appuntamenti ecc.
- Esci dalle chat di gruppo dove la tua presenza non è necessaria e cancella i membri inattivi dalle chat di gruppo.
- Allenati a lasciare il telefono a casa o a spegnerlo quando vai a fare delle commissioni o in caso di piccole azioni, in modo da abituarti a non averlo con te.
- Inizia ogni assemblea decidendo se i dispositivi elettronici sono ammessi oppure no; in caso negativo, raccoglili e mettili in un luogo lontano da quello in cui avviene la conversazione.

Soprattutto:

> **Non mandare messaggi o fare chiamate in cui si parli di argomenti particolarmente sensibili. Non fotografare o riprendere**

contribuiscono in una certa misura alla tua sicurezza e quindi, se non li usi, perché non farlo?

Backup

Gli smartphone spesso includono delle funzionalità di backup automatico su un account cloud legato al telefono (iCloud per Apple e Google Drive per Android). Tempo fa, Apple ha sospeso i suoi piani di garantire backup criptati su iCloud a seguito delle pressioni dell'FBI, per cui i backup sui dispositivi Apple risultano non-criptati. Google, invece, offre una crittografia end-to-end dei backup che, secondo indagini esterne, fornisce notevoli garanzie di privacy nei confronti di Google stessa e delle forze dell'ordine. In più, alcune app possono avere i loro servizi di crittografia. Ad esempio, è importante notare che WhatsApp può fare il backup delle tue conversazioni sui suoi server il che rende molto meno sicuro l'uso di quest'app per le comunicazioni.

La nostra raccomandazione è di evitare i backup su Apple, mentre i backup su Google sono sicuri nella misura in cui non vi siano comunque prove incriminanti sul tuo telefono. Considerato che i dati che vengono inviati a terze parti potrebbero essere persi o distrutti anche se non vengono recuperati dalla polizia, dovresti prendere in cosiderazione di fare un backup periodico su un hard disk cifrato che tieni a casa o in qualche posto sicuro.

App di messaggistica

Le app di messaggistica rappresentano un'alternativa più sicura rispetto alle chiamate e agli SMS.

Crittografia

Le app di chat testuale e vocale offrono uno o due tipi di crittografia.

Si ha **crittografia client-server** quando il canale tra un client (es. il tuo telefono) e il server è criptato e protetto da intercettazioni o manomissioni. Il messaggio è decifrato e salvato sul server. Quando il messaggio è richiesto da un altro client (es. il telefono del tuo amico), viene nuovamente cifrato e inviato.

La crittografia end-to-end (E2E) prevede che i client generino chiavi crittografiche e si scambino le chiavi pubbliche tra loro. I messaggi sono cifrati usando la chiave pubblica del client di destinazione e inviati tramite il server, che agisce come un ripetitore cieco, in quanto il messaggio è decifrabile solo dall'altro client.

La crittografia E2E fa si che un server o entità esterno tra il tuo telefono e quello della persona con la quale stai comunicando non possa leggere o alterare il messaggio inviato. Un agente malevolo può però ottenere informazioni dai metadati relativamente alla dimensione del messaggio, all'orario di invio, al mittente e al destinatario.

Alcune app di messaggistica offrono crittografia E2E ad attivazione, come Telegram con le sue chat segrete, ma questa funzionalità non è disponibile per le chat di gruppo. Altre app come Signal o Wire impiegano tassativamente la crittografia

E2E, così come iMessage (Apple) e WhatsApp.[20] Alcune app come Element hanno la crittografia E2E abilitatà di default, ma può essere disattivata per garantire la compatibilità con i client più vecchi.

La sicurezza della crittografia E2E dipende dalla verifica delle chiavi scambiate, che è spesso effettuata scansionando un QR code contenente la fingerprint che è unica e identifica la tua chiave di cifratura generata. Alcune app richiedono di verificare solo una fingerprint per tutti i dispositivi. Altre inviano una notifica nella conversazione quando l'impronta digitale del tuo contatto cambia, suggerendo un cambio di telefono o qualcosa di strano per cui è meglio verificare se è avvenuto un cambio di telefono o una reinstallazione. Altre app sfortunatamente non verificano questo cambio.

Consigliamo quindi di verificare tutte le impronte digitali di tutti i dispositivi e se per caso una cambia, dovresti riverificarla, altrimenti tutta la tua sicurezza potrebbe essere a rischio di qualche altra persona che sta usando il numero del tuo amico con un altro telefono. Inoltre, alcune app di chat non condividono i dati (messaggi e media) se non hai verificato la fingerprint con gli altri dispositivi nello stesso gruppo, per condividere i dati bisogna di verificare la fingerprint di tutti i dispositivi dei contatti appartenenti al gruppo.

2B **C6** DE **D5** 12
CF **B0** 69 **10** 56
8C **FB** 1D **8F** 60
B5 **03** 1D **60** B5

Figura 1: QR Code e impronte digitali

Utilizzo

Il mantra "usa solo Signal" è spesso ripetuto da ogni attivista, ma presuppone erroneamente che tutte le persone siano soggette alle stesse minacce. In alcune regioni, l'uso di Signal può essere bloccato dai firewall di Stato e il suo uso può essere talmente raro che un utente risulti automaticamente sospetto. In Nord America ed Europa, questi problemi generalmente non ci sono. Tuttavia, vi sono lamentele diffuse nei confronti di Signal come il fatto che necessiti di un numero di telefono per registrarsi e che la lista di contatti sia condivisa con il server in modi non troppo sicuri, che permettono di scoprire i contatti e lo scambio iniziale delle chiavi.

[20] Ci sono altre app di chat peer-to-peer rilevanti come Biar e Cwtch, che hanno metadati molto resistenti e possiedono altre funzionalità di sicurezza interessanti, ma che sono scarsamente utilizzate. Sono anche disponibili per iOS, il che spinge molte persone a non usarle per le comunicazioni sicure.

Potresti avere bisogno di trovare un telefono pubblico o convicere un estraneo alla stazione dei treni a prestarti il suo telefono per qualche minuto. Quando diciamo che un telefono usa e getta può essere usato per una sola azione, intendiamo "una sequanza di attività in un lasso di tempo limitato". Questo può significare un'azione diretta che ha luogo in sole due ore. Può anche significare la pianificazione e il coordinamento nel mese precedente all'azione così come durante l'azione stessa.

Con un utilizzo particolarmente attento, un gruppo chiuso può riutilizzare i suoi telefoni usa e getta per azioni ricorrenti. In questo caso, i telefoni devono essere usati in lotti cosicché i cicli di utilizzo dei dispositivi non si sovrappongano tra di loro.

Un fattore non vincolante, ma caldamente consigliato è che il telefono non sia acquistato immediatamente prima dell'azione. Questo crea possibilità aggiuntive che eventuali filmati di sicurezza del luogo di acquisto siano disponibili per le forze dell'ordine.

Cercare di nascondere l'esistenza del ciclo chiuso tra i telefoni può aiutare a impedire l'identificazione del gruppo. Un passo è non attivarli tutti in un breve lasso di tempo. L'attivazione graduale è meno riscontrabile quando lo Stato analizza i dati. Fai alcune chiamate da luoghi casuali a numeri che qualcuno chiamerebbe di solito, ma non parlare se qualcuno risponde. Chiama numeri con tempi di attesa ragionevolemente lunghi come banche o compagnie di assicurazione. Chiama un po' di negozi locali prima che aprano o dopo la chiusura. Queste false telefonate potrebbero non essere necessarie, dal momento che molti utenti in certe regioni non effettuano mai chiamate e utilizzano i loro piani dati per tutto. Data l'attenzione con cui un telefono usa e getta deve essere acquistato e usato, è altamente improbabile che valga gli sforzi. Se pensi che la tua azione necessiti di un telefono usa e getta, dovresti quasi certamente provare a cercare un modo per compiere l'azione senza alcun telefono. Per aiutare a chiarire ad ogni persona che un telefono usa e getta deve avere queste proprietà, evita di chiamarlo telefono usa e getta o e utilizza il termine demo o prepagato, se possibile.

Riduzione controllata

Questa zine tratta principalmente di caratteristiche ideali per un utilizzo sicuro del telefono, ma spesso questi ideali non sono raggiungibili. Un esempio di questo si ha se ti stai organizzando con persone che non si possono permettere uno smartphone. Comprare dei telefoni economici per una rete di persone che vogliono organizzare un'azione o anche semplicemente per coordinare degli incontri periodici può essere più facile e più gestibile finanziariamente che fare lo stesso con degli smartphone. Sfortunatamente, la mancanza di app di chat cifrate implica una sorveglianza più stringente per i tuoi messaggi.

Per evitare che lo Stato ottenga troppe informazioni sulle tue azioni, conviene affidarsi a soluzioni umane anziché tecniche. Un accordo per discutere esclusivamente degli orari e dei luoghi di incontro con un quantitativo essenziale di informazioni può ridurre le informazioni raccolte al minimo. Un semplice cifrario che rimpiazzi frasi comunemente utilizzate nell'organizzazione con frasi in codice casuali e inno-

agiscono o quando oltrepassano il confine. Questi dispositivi hanno dati privati minimi e sono considerati inaffidabili, a causa della possibilità di poterci installare un malware, quando in mano alle forze dell'ordine. Questi telefoni non sono usati per l'anonimato. Possono condividere una SIM card con quella utilizzata tutti i giorni e possono essere usati in un modo che li geolocalizzi nella residenza dell'utilizzatore. I telefoni demo forniscono pochi dati su messaggi o uso dell'account alla polizia nel caso vengano sequestrati. Non ci sono vincoli sul fatto che i telefoni demo e prepagati siano telefoni semplici. In molti casi sono smartphone perché questo permette agli utenti di avere mappe e comunicazione criptata E2E.

Chi fa attivismo erroneamente utilizza la formula "telefoni usa e getta" per descrivere i telefoni demo, i prepagati o qualsiasi telefono semplice.[22] Un telefono usa e getta prende il nome dal fatto che può essere utilizzato una sola volta, dopodiché di distrugge. Sono acquistati quando chi li usa ha bisogno di avere molteplici comunicazioni durante il corso dell'azione che porterà a un'indagine investigativa su larga scala. Perché un telefono sia usa e getta deve rispettare i seguenti criteri:

1. Il telefono deve essere acquistato in contanti[23].
2. La SIM card usata deve essere stata pagata in contanti.
3. Il telefono e la SIM card devono essere stati comprati da una persona che non ha altri telefoni o dispositivi tracciabili sulla sua persona al momento dell'acquisto.
4. Il telefono e la SIM card devono essere usati solo in combinazione tra loro.
5. Il telefono non deve mai essere portato in luoghi associati con l'utilizzatore a meno che non sia contemporaneamente spento e in un una gabbia di Faraday.
6. Il telefono non deve essere mai usato in presenza di telefoni non usa e getta o altri dispositivi che possono essere ricondotti all'utilizzatore o ai suoi associati.
7. Ogni account sul telefono deve essere fatto anonimamente, usato solo da quel dispositivo e mai più.
8. Il telefono deve essere usato per una e una sola azione.
9. Il telefono deve contattare solo altri telefoni usa e getta o parti non affiliate (es. un ufficio o l'obiettivo dell'azione).
10. Il telefono e la SIM card devono essere disattivati al termine dell'azione e distrutti immediatamente.

Un elemento che complica le cose è che alcuni telefoni o SIM card richiedono un'attivazione tramite chiamata a un numero o accedendo al sito del provider. In alcuni casi, questi siti bloccano le connessioni Tor. Usare una telefono non usa e getta per attivare la SIM card è una palese violazione del protocollo di sicurezza.

[22] Sembra che la gente utilizzi la formula "telefono usa e getta" perché suona "mega illegale" e "super criminale" e non perché stanno descrivendo le proprietà di un telefono usa e getta.

[23] Il furto di un telefono con una SIM attivata non è generalmenete consigliato perché ogni furto crea un data point di localizzazione aggiuntivo che può essere collegato all'azione, il telefono potrebbe non essere sbloccato e chi possiete il telefono potrebbe aver inserito il dispositivo nella lista nera gestita dagli operatori per evitare che riceva o effettui chiamate o utilizzi i dati mobili.

Per la maggior parte delle app, quando i messaggi sono ricevuti, vengono decifrati e salvati in chiaro sul dispositivo. Alcune app, come Signal, permettono di impostare una password per prevenire l'acceso ai messaggi mentre qualcun altro sta usando il telefono, ma ciò non cifra doppiamente i messaggi in alcun modo. Se la crittografia del dispositivo è abilitata, puoi riottenere un po' di privacy su quei messaggi, come descritto nella sezione dedicata alla crittografia.

Dal momento che i messaggi sono salvati in chiaro e possono essere recuperati anche con la crittografia del dispositivo, potresti ragionevolmente voler abilitare i messaggi temporanei (a scomparsa). Su alcune app, qualcuno può abilitare i messaggi temporanei per tutti i membri della chat. Su altre app, ogni persona deve attivare la funzionalità per assicurare che i messaggi scompaiano effettivamente dopo il tempo stabilito. Anche se può essere scomodo avere messaggi temporanei, dato che immagini, file o messaggi sono disponibili solo per l'ultima settimana o mese, ma è sicuramente preferibile rispetto all'avere un registro pluriennale di tutto ciò che hai detto o pensato e, in particolare, di tutti i posti che dici di aver attraversato.

Questo significa che dovresti decisamente preferire app di chat testuali e vocali che utilizzano tassativamente la crittografia E2E, a meno che non ci sia una ragione di sicurezza stringente per non farlo, dovresti verificare le chiavi prima di messaggiare e dovresti probabilmente abilitare i messaggi temporanei.

Non basta usare solo Signal

Diverse organizzazioni per la privacy e che fanno attivismo e si occupano di questi temi ogni giorno hanno fatto un lavoro eccellente nell'incoraggiare l'adozione di Signal tra le persone comuni e specialmente con ogni attivista. Hanno fatto un lavoro forse fin troppo buono, al punto che molte persone l'hanno interpretato come "se usi Signal, sei totalmente al sicuro". Questo ha portato alcune persone a discutere di questioni di cui non dovrebbero assolutamente parlare utilizzando dispositivi elettronici, assumendo erroneamente di essere a posto perché usano Signal. Tutte le contromisure di sicurezza si basano su di un insieme di assunti, da cui possono derivare dei rischi espliciti o cose che sono fuori ambito. Signal è piuttosto buona nel prevenire che gli attori statali usino la sorveglianza di massa per leggere i contenuti dei messaggi di testo. Nasconde persino alcuni—non tutti—metadati. Altre app di chat hanno modelli di rischio pressoché uguali. Tuttavia, se il tuo telefono è compromesso da un malware perché hai attirato attenzioni indesiderate o semplicemente perché la fortuna non è dalla tua parte, Signal non impedirà che le tue comunicazioni possano essere lette[21].

Per alcune lingue, in particolare quelle basate sui caratteri e non sulle lettere, gli editor del metodo di input (IME) vengono usati per convertire sequenze di lettere dell'alfabeto latino nei caratteri della lingua di destinazione. Questo viene fatto

[21] Inoltre, alcuni hanno adottato pratiche di sicurezza assurde, come entrare in varie chat di gruppo su Signal e discutere delle propore azioni senza accertarsi di chi fossero le altre persone nel gruppo. Non importa quanto buona sia la crittografia se una persona all'interno del gruppo è un infiltrato o una spia, non sei al sicuro.

Figura 2: Metodo di input e risultati in Pinyin

generalmente da app di terze parti installate sul dispositivo. Signal non è stata in grado di avvisare adeguatamente gli utenti che utilizzano gli IME sulla possibilità che le loro chat possano essere lette dal software stesso e riportate allo Stato prima che i messaggi siano cifrati.

Signal non è garanzia di sicurezza. Lo stesso vale per qualsiasi altra app di messaggistica che utilizza la crittografia E2E. Non le considerate tutte uguali.

Sebbene vi siano forti critiche nei confronti di Signal, questo è dovuto alla sua popolarità e ai fraintentimenti sul suo riguardo. Al momento in cui si scrive, è ancora una di un ristretto numero di app di chat cifrate che offrono un buon livello di sicurezza.

E-mail

Ci sono modi per rendere le comunicazioni via e-mail più sicure, ma l'e-mail come protocollo e mezzo di comunicazione è tendenzialmente poco sicura per le comunicazioni private. Gestori e-mail di nicchia e vicini alle esigenze di chi fa attivismo (es. autistici.org, riseup.net, ecc.) offrono significativi benefici di sicurezza contro le intercettazione da parte delle forze dell'ordine o hacker. Quando mandano le e-mail, alune persone utilizzano PGP o S/MIME, ma sono difficili da usare e non hanno una buona esperienza utente. Due persone che utilizzano questi mezzi di crittografia possono avere una protezione piuttosto buona contro le intercettazioni, ma un click sbagliato può inviare l'intera cronologia della conversazione in chiaro, rendendola leggibile dalle forze dell'ordine. ProtonMail ha fatto annunci audaci sulla crittografia per le sue e-mail e i suoi client e molte persone hanno inteso queste mezze verità come se usare un account ProtonMail significasse che tutte le proprie e-mail fossero cifrate, ma non è questo il caso.

Le e-mail dovrebbero essere tendenzialmente evitate per pianificazioni e in particolare per comunicazioni sicure. Detto questo, l'e-mail rimane popolare perché ogni dispositivo può ricevere e inviarle e alcune persone non vogliono o non usano smartphone. Per coordinare associazione degli affittuari o stabilire i turni al punto informazioni locale, le e-mail possono andare bene. Se scegli di usare le e-mail, parti dal presupposto che le forze dell'ordine stanno leggendo tutti i messaggi e mantieni la conversazione al minimo. Non trattare di attività illegali. Non discutere di dettagli succosi che possono essere sfruttati dallo Stato.

Infine, ci sono casi legittimi dove le e-mail e PGP possono essere l'ultima risorsa come un canale criptato utilizzato una tantum da qualcuno in fuga, in modo da stabilire un secondo canale di comunicazione più sicuro. In casi come questo, i telefoni dovrebbero essere evitati per la loro facile tracciabilità.

Più profili, più telefoni

A seconda del tuo modello di minaccia, potresti scegliere di mantenere più telefoni collegati a diversi account. Ad esempio, potresti avere un telefono per le tua vita pubblica, con gli account dei social media che usi per sentire la tua famiglia e un secondo telefono con una SIM separta e account distinto legato alla tua vita da attivista. Questa separazione degli account è parte di un processo chiamato compartimentalizzazione.

Il primo beneficio è che l'uso di diversi dispositivi per ciascuno dei tuoi profili previene che errori di programmazione o errori dell'utente possano far trapelare le tue informazioni private. Le app sul tuo telefono potrebbero avere comportamenti imprevisti come ad esempio mandare alla tua intera lista di contatti una richiesta di collegamento quando ti registri su un app di messaggistica. Potresti fare l'errore di rispondere a un post sui social media dall'account sbagliato. Quando clicchi su un indirizzo e-mail con l'intezione di usare uno dei tuoi alias, il sistema operativo del tuo telefono potrebbe iniziare a comporre l'e-mail con un client di default legato ad un altro alias e far scoprire un altra identità.

Il secondo beneficio è che il tuuo dispositivo da attivista può essere minimale e usato esclusivamente per comunicazioni sicure. Ogni app che installi è un possibile canale di ingresso per un malware, per cui se il tuo telefono ha solo il sistema operativo e due app di chat, è più difficile da compromettere. Usare molteplici telefoni di per sé non impedisce alle forze dell'ordine di collegare i tuoi account. Se porti con te i telefoni nello stesso momento o li usi negli stessi luoghi, possono essere collegati tra loro.

Come alternativa all'uso di più telefoni, puoi ridurre parte del rischio di fuoriuscta di dati a causa di errori o comportamenti imprevisti creando molteplici profili sul tuoi dispositivo Android. Questo non ti proteggerà dai malware, ma ti fornirà un po' di protezione. Uno dei casi più comuni per cui si hanno più telefoni è per organizzare un sindacato. Alcune aziende prevedono che le app siano installate da remoto come mezzo per proteggere la proprietà intellettuale o per mitigare le falle nella sicurezza. Queste sono app spyware e possono controllare completamente il tuo telefono. A parte questi casi, molte società impongono un'app di chat per le comunicazioni. Dovresti evitare di organizzare attività sindacali sui dispositivi aziendali o su quelli con spyware aziendali installati e dovresti evitare di utilizzare la chat aziendale per attività di sindacalizzazione.

Telefoni usa e getta, demo e prepagati

Molte persone comprendono l'importanza dei loro telefoni e sanno che possono essere tracciati tramite essi o che la loro perdita può essere devastante. Vi sono diversi approcci utilizzati da chi fa attivismo per aiutare a ridurre il rischio anche se non sono in grado di spiegarlo completamente o non sanno perché le loro contromisure funzionino. Alcune persone hanno telefoni demo o prepagati che si portano quando