Guida all'OPSEC: Modelli di minaccia, sicurezza operativa e privacy

> *"Sostenere che non ci importi del diritto alla privacy perché non abbiamo nulla da nascondere non è diverso dal dire che non ci importi della libertà di parola perché non abbiamo nulla da dire." — Edward Snowden*

Modello di minaccia: Chi ci dà la caccia?

Prima di muovere anche solo un dito, dobbiamo capire contro chi ci stiamo difendendo. L'OPSEC (Operational Security) non è una lista magica di regole da seguire alla cieca. Si tratta di compiere mosse calcolate in base ai nostri rischi specifici. Non basta installare una VPN a caso e considerarsi a posto: questo è il modo di fare dei dilettanti allo sbaraglio. Dobbiamo costruire le nostre difese basandoci su chi ci sta cercando, cosa vuole e cosa succede se riesce a prenderci.

Cosa stiamo proteggendo?

Stiamo difendendo dati personali sensibili, informazioni aziendali riservate, attività non proprio legali o semplicemente il nostro sacrosanto diritto alla privacy? Magari siamo giornalisti, attivisti, hacker o solo persone che vogliono tenere le proprie cose sotto chiave. Asset diversi richiedono livelli di protezione diversi.

Chi ci dà la caccia?

Qui le cose si fanno serie. C'è una differenza abissale tra l'evitare un ragazzino dispettoso su un forum e lo schivare un'operazione di sorveglianza governativa in piena regola. Ecco lo spettro delle minacce, in breve:

- **Livello Basso**: Amici ficcanaso, ex partner, troll della domenica, script kiddie senza arte né parte.

- **Livello Medio**: Concorrenti commerciali, cybercriminali, doxxer, stalker.
- **Livello Alto**: Forze dell'ordine, agenzie di intelligence, spionaggio industriale, apparati statali.

Ognuno di questi attori opera in modo diverso. Alcuni si affidano all'ingegneria sociale, altri usano exploit tecnici, altri ancora sfondano la porta sfruttando il potere legale. Più il nostro nemico è potente, più la nostra OPSEC deve essere priva di crepe.

Cosa succede se vincono loro?

Questo è il costo del fallimento. Qual è lo scenario peggiore se i nostri dati, la nostra identità o la nostra posizione finiscono nelle mani sbagliate? Rimanere doxxati e tormentati? Perdere l'accesso ai nostri account e ai nostri beni digitali? Finire sotto processo, in galera o peggio? Se le conseguenze possono stravolgerci la vita, vediamo di non giocare. È qui che entrano in gioco la compartimentazione, l'anonimato e i protocolli di sicurezza più rigidi.

Costruire la difesa

Il modello di minaccia non è un esercizio teorico: detta ogni singola decisione della nostra OPSEC. Se la nostra minaccia più grande è qualcuno che cerca di sbirciare i nostri messaggi, non ci serve la sicurezza della NSA. Ma se abbiamo contro uno Stato, le regole devono essere ferree.

Prima di applicare qualsiasi misura di sicurezza, mappiamo il nostro modello di minaccia:

- Cosa stiamo proteggendo?
- Chi ci dà la caccia?
- Qual è la cosa peggiore che potrebbe accadere?
- Quali risorse e capacità ha il nostro avversario?

Solo quando abbiamo risposte chiare a queste domande possiamo iniziare a strutturare una strategia di sicurezza che funzioni davvero. Tutto il resto è solo teatro della sicurezza.

Stilometria: La minaccia invisibile all'anonimato

La stilometria è una tecnica utilizzata per analizzare i pattern di scrittura al fine di identificare l'autore, anche quando si usa uno pseudonimo. Può tracciare i nostri post, le nostre email e i nostri commenti sui social media attraverso diverse piattaforme, anche se pensiamo di essere anonimi. Elementi come la struttura delle frasi, la scelta delle parole e le abitudini di punteggiatura creano un'impronta digitale unica che può essere ricondotta a noi. Se il nostro stile di scrittura può essere identificato, lo stesso vale per la nostra identità.

Come combattere la stilometria

Per proteggerci, possiamo creare uno stile di scrittura unico da associare esclusivamente alla nostra identità anonima. Iniziamo analizzando le nostre abitudini di scrittura naturali: osserviamo il nostro vocabolario, la struttura delle frasi e il tono. Una volta individuati i pattern che potrebbero tradirci, cambiamoli deliberatamente.

Ad esempio, se il nostro stile di scrittura tradisce che siamo videogiocatori di 25 anni, modifichiamolo per sembrare quarantenni con un'esperienza di vita completamente diversa. La chiave è la costanza. Adottiamo questo nuovo stile in tutte le comunicazioni sotto quello pseudonimo. Un singolo errore di tono o di lessico può farci saltare la copertura.

Ricordiamo che, nonostante i nostri sforzi, è facilissimo scivolare di nuovo nello stile di scrittura naturale. Se uno strumento stilometrico rileva incongruenze, può ricostruire il nostro stile originale e risalire alla nostra vera identità.

Inoltre, le tecniche di deanonimizzazione basate sull'intelligenza artificiale rappresentano oggi una minaccia ancora più grande. L'IA può analizzare enormi set di dati per trovare correlazioni sottili, come tempi di pubblicazione, posizioni geografiche o frasi ricorrenti tra piattaforme diverse, collegando account che sembrano non avere nulla in comune.

> ***Consiglio**: Evitiamo le comunicazioni in tempo reale (chat live) il più possibile: è lì che è più facile fare un passo falso e rivelare la propria identità o il proprio stile di scrittura. Scriviamo i nostri messaggi prima su un editor di testo offline (come Blocco Note), modifichiamo il nostro stile con calma e solo allora incolliamolo e pubblichiamolo.*

Costruire un Alias: Creare un'identità fittizia credibile e sicura

Creare una nuova identità non significa mettere insieme dettagli a caso: dobbiamo costruire un personaggio credibile. Partiamo dalle basi come nome, età e posizione geografica. Quindi, creiamo un'email dedicata esclusivamente a questo alias, evitando di usare qualsiasi elemento riconducibile alla nostra vita reale.

Per riempire i dettagli vuoti, possiamo usare strumenti come il *Fake Person Generator* (https://www.fakepersongenerator.com). Per le foto del profilo, evitiamo assolutamente immagini d'archivio o stock: usiamo strumenti di IA generativa come *Stable Diffusion* o *Midjourney* per creare volti realistici ma inesistenti.

Assicuriamoci che non ci sia alcuna sovrapposizione tra la nostra identità reale e quella fittizia. Facciamo attenzione ai minimi dettagli: abitudini, orari o scelte di parole che potrebbero collegare le due vite. Più siamo meticolosi, più sarà difficile per chiunque unire i puntini.

Profilazione comportamentale e biometrica

Quando cerchiamo di rimanere anonimi online o gestiamo più identità, non conta solo *cosa* scriviamo, ma anche *come* lo scriviamo. Anche sotto rete Tor, la nostra anonimizzazione può essere compromessa dalla profilazione comportamentale e biometrica. Il modo in cui interagiamo con i nostri dispositivi (la velocità di battitura, gli intervalli tra

i tasti e persino i movimenti del mouse) può rivelare molto più di quanto immaginiamo. Siamo imprevedibili.

Grazie ai progressi dell'intelligenza artificiale, la profilazione comportamentale non si limita più ai soli dati fisici di input. Anche le abitudini di navigazione, la durata delle sessioni e i metadati possono essere analizzati tra le piattaforme per deanonimizzare gli utenti. L'IA eccelle nel rilevare pattern invisibili all'occhio umano.

Cos'è la profilazione della digitazione?

È una tecnica di tracciamento basata sulla dinamica di digitazione (*keystroke dynamics*), in particolare sul tempo che intercorre tra la pressione di un tasto e l'altro. La ricerca dimostra che il ritmo e la durata della digitazione sono unici come un'impronta digitale. Agli algoritmi bastano pochi minuti di misurazione per identificare una persona, anche se cambia browser, indirizzo IP o sito web. Questa è una minaccia diretta per gli utenti Tor.

Il rischio aumenta quando gli stessi pattern vengono registrati su più siti. I tracciatori possono confrontare e collegare le identità, associando nickname o account diversi alla stessa persona fisica. Non sono solo i proprietari dei siti a raccogliere questi dati: anche i circuiti pubblicitari integrano script JavaScript specifici per catturare i tempi di digitazione. Molti istituti bancari utilizzano già questa tecnologia per rilevare frodi analizzando i pattern di accesso.

Come limitare la profilazione della digitazione

Se preoccupa questo tipo di tracciamento, si possono adottare queste contromisure:

1. **Scrivere offline su un editor di testo**: Compiliamo i nostri testi offline su Blocco Note, quindi copiamo e incolliamo il risultato nel browser. Questo impedisce al sito web di registrare gli intervalli di digitazione in tempo reale. Se questa pratica diventa di uso comune, rende la profilazione molto più complessa.
2. **Usare estensioni del browser**: Alcune estensioni tentano di offuscare la dinamica di digitazione introducendo ritardi casuali nella pressione dei tasti. Tuttavia, facciamo attenzione con i

browser basati su Chromium (come Chrome), poiché i siti web possono bypassare o disattivare tali estensioni.

3. **Disattivare JavaScript**: Questa è la misura più drastica ma efficace. Senza JavaScript attivo, i siti web non possono eseguire gli script che registrano i tempi di digitazione. Teniamo conto, però, che in futuro potrebbero emergere tecniche che non necessitano di JS.

Blindare i Social Media: Ridurre al minimo l'impronta digitale

---

Diciamoci la verità: evitare del tutto i social media oggi è quasi impossibile, a meno che non si decida di andare a vivere in un bosco. Ma questo non significa che dobbiamo regalare la nostra vita. Possiamo ridurre al minimo il disastro seguendo queste regole:

- **Eliminare i vecchi account** e crearne di nuovi usando esclusivamente Tor. Se serve un numero di telefono temporaneo per la verifica, ricordiamo che questi servizi lasciano una traccia finanziaria: per rimanere anonimi paghiamo in Monero (XMR) su siti come https://www.smscodes.io o https://crypton.sh.
- **Disattivare tutte le opzioni di condivisione dati** e quelle impostazioni camuffate sotto la dicitura "*migliora la tua esperienza utente*".
- **Rendere tutti i nostri profili privati**.
- **Non usare mai il nostro vero nome**, le nostre foto o informazioni personali tra le piattaforme. Se possibile, usiamo dispositivi o macchine virtuali (VM) separate per ciascun alias, per evitare il tracciamento tramite fingerprinting del dispositivo.
- **Per l'immagine del profilo**, non usiamo foto personali o immagini che possano rivelare dettagli sulla nostra posizione (come una foto scattata dalla finestra di casa nostra).
- **Non inserire dettagli personali** come età, hobby o interessi nella biografia. Lasciare questi campi vuoti è la scelta più sicura.
- **Rimuovere la geolocalizzazione** da tutti i post e dalle immagini.
- **Evitare di accettare richieste d'amicizia** o follower da sconosciuti.
- **Attivare l'autenticazione a due fattori (2FA)** su ogni singolo account, usando applicazioni offline come *Aegis* o *FreeOTP*.

- **Usare username diversi su ogni piattaforma** per impedire a strumenti di OSINT come `whatsmyname.app` di mappare la nostra presenza sul web.
- **Usare password forti e uniche** per ogni servizio, generate casualmente.

Password forti: Come evitare le trappole comuni

Se riutilizziamo la stessa password su più piattaforme, stiamo rendendo il lavoro di tracciamento incredibilmente facile. Le password devono essere uniche per ogni singolo account. Un password manager come **KeePassXC** ci permette di generare e salvare credenziali forti in un database cifrato locale. Per una sicurezza ancora maggiore, gestiamo il database su una macchina virtuale offline (come Whonix) per prevenire qualsiasi fuga di dati. Se generiamo password manualmente, usiamo strumenti come `pwgen` o il metodo *Diceware*.

Pagamenti anonimi

Nel mondo dei pagamenti digitali, **Monero (XMR)** è l'unica scelta seria grazie a un'architettura crittografica che nasconde per impostazione predefinita il mittente, il destinatario e l'importo della transazione. Ecco come procurarsi Monero senza lasciare tracce:

Opzione 1: Exchange Peer-to-Peer (P2P) senza KYC

Usiamo piattaforme P2P come BitValve, HodlHodl o LocalCoinSwap che consentono l'acquisto di crypto senza richiedere documenti d'identità (KYC). Possiamo acquistare una criptovaluta più comune (come Litecoin o Bitcoin) e poi usare un servizio di swap anonimo come **Trocador** per scambiarla con Monero, inviando i fondi direttamente al nostro wallet personale.

Opzione 2: Exchange Decentralizzati (DEX)

Possiamo acquistare Monero direttamente su mercati decentralizzati come Bisq o Haveno. Non richiedono KYC, operano direttamente tra acquirenti e venditori e ci permettono di prelevare i fondi sul nostro wallet personale senza intermediari.

Accortezze fondamentali:

- **Wallet personale**: Inviamo sempre i nostri fondi a un wallet Monero di cui possediamo le chiavi private, preferibilmente configurato su una macchina sicura (un hardware wallet o un dispositivo isolato dalla rete - *air-gapped*).
- **Dispositivi dedicati**: Per transazioni finanziarie critiche, non usiamo i nostri dispositivi personali. Prevediamo una macchina pulita e dedicata, come un portatile configurato con Qubes OS + Whonix.
- **Spesa anonima**: Per gli acquisti online, usiamo mercati che accettano Monero direttamente. Possiamo usare Trocador per acquistare carte regalo prepagate pagando in XMR, garantendoci un ulteriore livello di privacy.

Connessione alla rete Monero: 3 strade a confronto

1. **Nodo remoto (tramite Whonix)**: È la scelta più comoda. Offre una buona sicurezza se usata sotto Whonix per evitare la fuga dell'indirizzo IP. Possiamo trovare nodi remoti su portali come https://monero.fail/, tenendo conto dei rischi di tracciamento da parte di nodi malevoli.
2. **Nodo locale**: Teoricamente è l'opzione più sicura, ma richiede di scaricare l'intera blockchain sul nostro computer (centinaia di gigabyte). Farlo sotto rete Tor è lentissimo, e farlo in chiaro rivela al nostro operatore che usiamo Monero. Inoltre, a ogni riavvio dovremo attendere la sincronizzazione.
3. **Nodo VPS dedicato**: Consiste nel far girare un nodo Monero su una VPS connessa alla rete clearnet (che mantiene aggiornata la blockchain), a cui ci connettiamo esclusivamente tramite un servizio Onion di Tor per interrogare il wallet in sicurezza.

Gestione intelligente dei guadagni

Se otteniamo dei **vaìni** (guadagni) da attività legate a Tor o a progetti anonimi, la prima regola d'oro è: **teniamo un profilo basso**. Evitiamo qualsiasi sfoggio vistoso di ricchezza. Comprare auto di lusso, immobili o beni costosi è il modo più rapido per farsi notare dai controlli fiscali o dalle forze dell'ordine. Tenere questi guadagni fuori dal sistema bancario tradicional è fondamentale per

preservare l'anonimato. Accumuliamo contanti in un luogo sicuro per le emergenze.

Integriamo questi fondi nella nostra vita quotidiana in modo impercettibile: facciamo piccoli miglioramenti, acquistiamo beni di consumo comune o attrezzature da lavoro che si fondano con le nostre spese abituali. Usiamo il contante il più possibile per evitare tracciamenti e prediligiamo scontrini generici alle fatture intestate.

Navigazione Web: Manteniamo intatta la nostra privacy

I browser commerciali più diffusi (come Chrome o Opera) sono idrovore di dati personali. Per migliorare la nostra sicurezza quotidiana, passiamo a browser orientati alla privacy come **LibreWolf** o **Brave**.

Se dobbiamo gestire più profili o identità fittizie contemporaneamente, la soluzione migliore sono gli *anti-detection browser* come Dolphin{anty}, Incogniton o Ghost Browser, progettati per mascherare le impronte digitali dei dispositivi ed evitare il tracciamento incrociato.

- **Motori di ricerca**: Evitiamo Google e motori commerciali. Usiamo alternative che rispettano la privacy come **SearXNG** o **DuckDuckGo**.
- **Estensioni consigliate per la privacy**:
  - *uBlock Origin* (il blocco dei contenuti definitivo)
  - *NoScript* (per controllare l'esecuzione di JavaScript)
  - *Privacy Badger* (per bloccare i tracker invisibili)
  - *Cookie AutoDelete* (per eliminare i cookie alla chiusura delle schede)
  - *ClearURLs* (per rimuovere i parametri di tracciamento dagli indirizzi web)

Protezione dei dati ed eliminazione sicura

Quando eliminiamo un file dal nostro sistema, questo non scompare. Il sistema operativo si limita a marcare lo spazio occupato da quel file come "libero", ma i dati restano sul disco finché non vengono

sovrascritti da nuove informazioni. Se abbiamo memorizzato file sensibili senza cifratura, i loro frammenti resteranno rilevabili per molto tempo.

La soluzione migliore è utilizzare un file system cifrato fin dall'inizio. Se invece abbiamo già memorizzato file in chiaro e vogliamo eliminarli, dobbiamo usare uno strumento di cancellazione sicura (*shredder*) che sovrascriva lo spazio vuoto più volte (ad esempio seguendo lo standard NIST 800-88). Per operazioni sensibili, lavoriamo sempre all'interno di sistemi operativi live come **Tails** o configurazioni sicure come **Qubes OS + Whonix**.

Archiviazione cifrata: La chiave per proteggere i nostri dati

L'archiviazione cifrata è obbligatoria. Il sistema operativo genera costantemente file temporanei, log, swap e file di ibernazione che possono rivelare le nostre attività anche se abbiamo cancellato i file principali. Senza cifratura totale del disco, chiunque abbia accesso fisico alla macchina può estrarre questi dati.

Usiamo sempre software di cifratura open-source, dove il codice può essere verificato dalla comunità. Per sistemi Windows la scelta classica è **VeraCrypt**, mentre per gli utenti Linux lo standard di riferimento è **dm-crypt/LUKS**.

Sicurezza Mobile: Fortificare lo smartphone

- **Evitare gli iPhone**: Nonostante il marketing di Apple sulla privacy, l'ecosistema iOS è completamente chiuso e proprietario. Non possiamo sapere cosa viene raccolto in background, non possiamo verificare il codice e non possiamo ottenere i privilegi di root per controllare il sistema. Inoltre, il dispositivo è strettamente legato ai servizi iCloud.
- **Attenzione alle ROM generiche**: ROM come *LineageOS* sembrano attraenti per la privacy, ma spesso richiedono di lasciare il bootloader del telefono sbloccato. Questo rende il dispositivo vulnerabile a strumenti di analisi forense fisica (come

Cellebrite), che possono estrarre tutti i dati bypassando la cifratura se hanno accesso fisico al dispositivo.
- **La scelta sovrana: GrapheneOS**: Per il massimo livello di privacy e sicurezza, installiamo GrapheneOS (disponibile sui dispositivi Google Pixel, dal modello 6 in poi). Questa configurazione offre una cifratura eccellente e un hardware resistente agli attacchi forensi. Se abbiamo un budget ridotto, acquistiamo un dispositivo Pixel usato (pagato in contanti) e assicuriamoci di non inserire mai una SIM card precedentemente intestata a noi.

Comunicatori sicuri ed email: Proteggere le conversazioni

Per scambiare messaggi, usiamo applicazioni come **Signal** (o il suo fork avanzato **Molly**), **Session** o sistemi federati **XMPP** che offrono cifratura end-to-end (con OTR o OMEMO) e possono girare sotto rete Tor (onion service).

Se usiamo ancora Gmail, Outlook o simili per comunicazioni riservate, fermiamoci immediatamente: sono un disastro per la privacy. Spostiamoci su servizi email orientati alla sicurezza e che non richiedono dati personali, come *TorBox*, *cock.li* o *morke.org*.

E ricordiamoci: **PGP è nostro amico**. Impariamolo, usiamolo, viviamolo.

> ***Attenzione**: Diffidiamo dei servizi proprietari che promettono "sicurezza perfetta" o telefoni super-cifrati già pronti all'uso (come i vecchi Encrochat, Anom o Phantom Secure). Molti di questi si sono rivelati essere dei "honeypot" (trappole) creati o presi in gestione dalle forze dell'ordine per intercettare i criminali. Affidiamoci solo a soluzioni open-source, decentralizzate e ampiamente auditate.*

VPN: Sicure, ma non fidiamoci alla cieca

I servizi VPN commerciali vengono pubblicizzati come la panacea di tutti i mali della privacy. È per lo più marketing. Una VPN cifra il traffico tra noi e il loro server, ma il provider VPN vede comunque

tutto il nostro traffico in uscita. Come facciamo a essere sicuri che non tengano log, anche se dichiarano il contrario?

Se proprio dobbiamo sceglierne una, verifichiamo queste condizioni:

- **Politica No-Logs reale**: Deve essere stata verificata da audit indipendenti o casi giudiziari reali.
- **Pagamento anonimo**: Devono accettare pagamenti in Monero (XMR) senza richiedere email personali (come fa **Mullvad**).
- **Evitare le VPN gratuite**: Vendono i nostri dati per mantenersi.

Se vogliamo un controllo reale, possiamo noleggiare una VPS in una giurisdizione non collaborativa (come la Russia) e configurare il nostro server VPN personale, così saremo gli unici a gestire i log e la sicurezza dell'infrastruttura.

> ***Importante**: Ricordiamo che il nostro fornitore di servizi internet (ISP) non vedrà cosa facciamo, ma saprà comunque che siamo connessi a una VPN. Se abbiamo bisogno di anonimato assoluto e sicurezza a livello statale, consideriamo le VPN inutili o dannose. Usiamo le VPN per la navigazione quotidiana, ma passiamo a Tor/Whonix quando la posta in gioco si fa alta.*

Sicurezza di rete

La nostra rete domestica è il retrobottega della nostra vita digitale. Se viene violata, siamo finiti.

- **Eliminare i router degli ISP**: I router forniti dai gestori telefonici sono pieni di backdoor, firmware scadenti e vulnerabilità mai patchate. Sostituiamoli con un dispositivo che supporti firmware open-source (come un router GL.iNet o una scheda configurata con OpenWRT), flashato manualmente da una macchina offline fidata. Disattiviamo qualsiasi aggiornamento automatico non controllato da noi.
- **Configurare il firmware OpenWRT o OPNsense**: Modifichiamo immediatamente le credenziali di default. Disabilitiamo la gestione remota e l'accesso al pannello di amministrazione dalla porta WAN.
- **Isolare i dispositivi IoT**: Smart TV, assistenti vocali, termostati intelligenti e telecamere sono spie travestite da elettrodomestici. Comunicano costantemente con server cloud

esterni. Configuriamo una VLAN (Virtual LAN) dedicata esclusivamente a queste cianfrusaglie, separandole completamente dalla nostra rete di lavoro principale.
- **Configurare il firewall**: Applichiamo una politica restrittiva. Blocchiamo tutto il traffico in uscita per impostazione predefinita, autorizzando solo i servizi e le porte strettamente necessari.
- **Monitorare il traffico**: Impariamo a usare strumenti come *Wireshark*, *Suricata* o *Zeek*. Se notiamo connessioni sospette verso server sconosciuti o data center esteri non autorizzati, tagliamo la connessione immediatamente.
- **Risoluzione DNS sicura**: Evitiamo i DNS di Google (8.8.8.8) o Cloudflare (1.1.1.1), che registrano la nostra cronologia di navigazione. Usiamo servizi che rispettano la privacy come **Quad9** (9.9.9.9), i DNS di **Mullvad** (194.242.2.2) o configuriamo un server ricorsivo locale come *Unbound*. Cifriamo le richieste DNS tramite DNS-over-HTTPS (DoH) o DNS-over-TLS (DoT).
- **Cablaggio fisico**: Il Wi-Fi è insicuro per definizione. Se cerchiamo il massimo livello di sicurezza, usiamo cavi Ethernet. Se dobbiamo usare il Wi-Fi, configuriamo come minimo la sicurezza WPA3, usiamo un SSID (nome di rete) composto da caratteri casuali e disattiviamo assolutamente il WPS (Wi-Fi Protected Setup), che è una backdoor di fabbrica.

Tor e I2P

Se abbiamo bisogno di anonimato a livello di rete, dobbiamo usare **Tor** o **I2P**. Ma teniamo a mente che non sono magici:

- **Attacchi di correlazione temporale**: Se un avversario potente (come un'agenzia governativa) controlla sia il nodo di ingresso che quello di uscita della rete Tor che stiamo usando, può analizzare i tempi dei pacchetti e risalire alla nostra identità.
- **Nodi malevoli**: Molti nodi di uscita sono gestiti da agenzie di sicurezza o ricercatori per analizzare il traffico di transito. Non trasmettiamo mai dati in chiaro attraverso la rete Tor.
- **Configurazione del browser**: Disabilitiamo sempre JavaScript (JS) nel browser Tor per evitare exploit che potrebbero rivelare il tuo vero indirizzo IP.

Metadati e firme digitali nelle immagini

Quando scattiamo e condividiamo una foto, non stiamo inviando solo pixel. Inviamo una montagna di informazioni invisibili:

1. Dati EXIF

I metadati EXIF (Exchangeable Image File Format) sono incorporati nei file immagine e contengono informazioni sul modello della fotocamera, le impostazioni di scatto (diaframma, tempo, ISO) e spesso le coordinate GPS esatte di dove è stata scattata la foto. Rimuoviamo sempre i dati EXIF prima di pubblicare qualsiasi immagine online.

2. Rumore del sensore (PRNU)

Ogni sensore fotografico ha imperfezioni microscopiche uniche nel silicio. Questo crea un pattern di rumore digitale invisibile all'occhio ma rilevabile tramite algoritmi forensi. Questo pattern funge da vera e propria "impronta digitale" della fotocamera. Se pubblichiamo molte foto scattate con lo stesso telefono, un analista può collegarle tutte allo stesso sensore fisico.

3. Tabelle di quantizzazione

I file JPEG utilizzano tabelle di quantizzazione per comprimere l'immagine. Queste tabelle variano a seconda del software di editing o del modello di fotocamera utilizzato per salvare il file. Analizzando queste tabelle, gli esperti possono capire quale programma (o quale marca di dispositivo) ha generato l'immagine, smascherando tentativi di camuffamento.

OPSEC Fisica

La sicurezza digitale crolla miseramente se la nostra sicurezza fisica fa acqua.

1. Il "Covo dell'Hacker" (Workspace sicuro)

Creiamo uno spazio dedicato e inaccessibile per le nostre attività sensibili.

- **Computer fisso**: Usiamo una macchina dedicata che non esce mai da quella stanza. Rimuoviamo la batteria se si tratta di un portatile per renderlo un dispositivo puramente stazionario, evitando che venga smarrito o sequestrato in viaggio.
- **Spegnimento d'emergenza**: Installiamo un interruttore rapido (*kill switch*) per togliere l'alimentazione elettrica all'istante, avviando la cifratura forzata in caso di emergenza.
- **Isolamento dei segnali**: Usiamo gabbie di Faraday o buste schermate per riporre i telefoni o i dispositivi wireless quando non sono in uso, impedendo la localizzazione o attacchi remoti.
- **Accesso controllato**: Impediamo l'accesso alla stanza a chiunque. Usiamo generatori di rumore bianco per evitare intercettazioni acustiche passive.
- **Nessun incrocio di mondi**: Non usiamo i dispositivi di questo spazio per attività personali o quotidiane.

2. Spegnere sempre i dispositivi

La crittografia totale del disco non serve a nulla se si lascia il computer acceso o in modalità sospensione (sleep). In quello stato, le chiavi di decifrazione si trovano all'interno della memoria RAM e possono essere estratte tramite attacchi fisici (come il *cold boot attack*). Spegniamo sempre completamente la macchina quando non la usiamo.

3. Essere invisibili

Quando ci spostiamo, evitiamo abiti appariscenti, loghi di brand o accessori memorabili. Vestiamoci in modo neutro per confonderci tra la folla. L'anonimato inizia dal farsi dimenticare.

4. GPS e Wi-Fi pubblici: Zone vietate

Disattiviamo sempre la localizzazione GPS sui nostri dispositivi. Evitiamo di connetterci a reti Wi-Fi pubbliche o sconosciute: sono i terreni preferiti per attacchi di tipo Man-in-the-Middle (MitM) e intercettazione dei dati.

5. Triangolazione dei telefoni cellulari

La rete telefonica traccia la nostra posizione confrontando la distanza del telefono dalle celle telefoniche:

- **Una torre**: L'operatore sa in quale macro-area circolare ci troviamo rispetto all'antenna.
- **Due torri**: L'intersezione restringe il campo a due possibili aree.
- **Tre torri**: La trilateralizzazione individua la nostra posizione esatta con estrema precisione.

Nelle città, questo sistema può localizzarci nel raggio di pochi metri. Per evitare questo tracciamento, riponiamo il telefono in una custodia di Faraday schermata o, meglio ancora, lasciamolo spento a casa prima di effettuare operazioni riservate.

6. Archiviazione cifrata in viaggio

Se dobbiamo trasportare dati su chiavette USB o dischi portatili:

- Usiamo supporti dotati di asole per assicurarli al polso o all'interno della giacca.
- Colleghiamo i dispositivi tramite cavi corti e fragili che possano essere strappati o distrutti rapidamente in caso di necessità.
- Cifra sempre tutto con VeraCrypt o LUKS.

7. Confondere il riconoscimento facciale

In aree videosorvegliate, indossiamo occhiali da sole scuri non riflettenti, cappelli con visiera calata o sciarpe con pattern geometrici per confondere i sistemi di tracciamento biometrico. Evitiamo camuffamenti eccessivamente bizzarri che otterrebbero l'effetto opposto di farci notare.

8. Trasporti pubblici rispetto a veicoli privati

Per spostarci, preferiamo i mezzi pubblici ai veicoli di proprietà. Le auto private sono costantemente tracciate dai lettori di targhe autostradali (tutor) e dalle telecamere cittadine. Paghiamo sempre i biglietti in contanti per non lasciare tracce bancarie.

9. Protocolli di emergenza e fuga

- **Pulsante di autodistruzione (Kill Switch)**: Configuriamo script rapidi per chiudere tutte le sessioni attive e smontare i volumi cifrati all'istante.
- **Piani di evacuazione**: Pianifichiamo rotte di fuga e individuiamo luoghi sicuri dove rifugiarci se la nostra sicurezza fisica viene compromessa.
- **Abbandono dei dispositivi**: Se riteniamo di essere seguiti, spegniamo e abbandoniamo tutti i nostri telefoni. Molti dispositivi moderni continuano a trasmettere segnali di localizzazione anche da "spenti".

Difesa psicologica contro l'ingegneria sociale

L'ingegneria sociale non è una leggenda da film. Le agenzie di sicurezza e gli investigatori privati la usano regolarmente: da finti incidenti stradali a false notifiche di emergenza per farci uscire allo scoperto. La manipolazione e la diffidenza strategica sono strumenti di sopravvivenza.

1. Ingegneria sociale nella vita reale

- **False emergenze**: Incidenti stradali simulati, visite improvvise di finti agenti o chiamate urgenti da colleghi, vicini o manutentori per spingerci a compiere azioni affrettate.
- **Infiltrazioni fisiche**: Finti corrieri, tecnici della rete internet o addetti alle pulizie che cercano di accedere al nostro spazio di lavoro.
- **Honeytrap (Trappole di miele)**: Profili fittizi attraenti online che passano mesi a costruire un rapporto di fiducia con noi solo per raccogliere informazioni.
- **Quid Pro Quo**: Persone che ci offrono aiuto apparentemente disinteressato per farti sentire in debito e spingerci a ricambiare con informazioni riservate.

2. La mentalità paranoica

- **Cautela machiavellica**: Consideriamo la fiducia come una vulnerabilità sfruttabile. Assumiamo che ogni interazione inaspettata sia un tentativo di exploit.
- **Compartimentazione**: Non parliamo mai di lavoro o di attività riservate con amici o familiari. Non possono rivelare segreti che non conoscono.

Il trucco dello smalto con i glitter (Physical Tampering)

Se vogliamo proteggere l'integrità fisica dei nostri dispositivi (come le viti sul fondo del nostro portatile) per accorgerci se qualcuno li ha aperti a nostra insaputa mentre eravamo lontani, usiamo questo metodo economico ed efficace:

1. Acquistiamo dello smalto per unghie trasparente che contenga dei **glitter** (brillantini).
2. Applichiamo una piccola quantità di smalto sopra le viti di fissaggio del portatile, coprendole.
3. Scattiamo foto ad altissima risoluzione da diverse angolazioni una volta che lo smalto si è asciugato.
4. I glitter sospesi nello smalto trasparente si disporranno in una struttura tridimensionale completamente casuale e unica, impossibile da replicare.
5. Se qualcuno svita il portatile per installare un keylogger hardware (un keylogger fisico) e prova a rimettere lo smalto, la disposizione dei glitter non corrisponderà mai alle nostre foto originali.

Credits

- **Autore originale**: Zycher
- **Sito ufficiale**: https://whos-zycher.github.io/opsec-guide/
- **Repository GitHub**: https://github.com/whos-zycher/opsec-guide
- **Supporto all'autore**:
  - **XMR**: `84h9GeLKqoTXZMDBPysNs4Dbu1tqR9dtz3kAkLBguUPFF9BCGVQQBmr4Dr4aCqXm6KinwUS99GMxj86DAL`
  - **BTC**: `bc1q6n2kdjh2p4h2chmp7uj3937c8pcxd846d8hgnnp68vfh92dn03pqkw4vd9`

[Che il talpone sia con voi]

[EOF]

Fluxer Icon

Canale di discussione e supporto

Canale di discussione e supporto. Per confrontarti su configurazioni o altro entra su fluxer.dreadful.work (https://fluxer.dreadful.work/invite/dreadful).