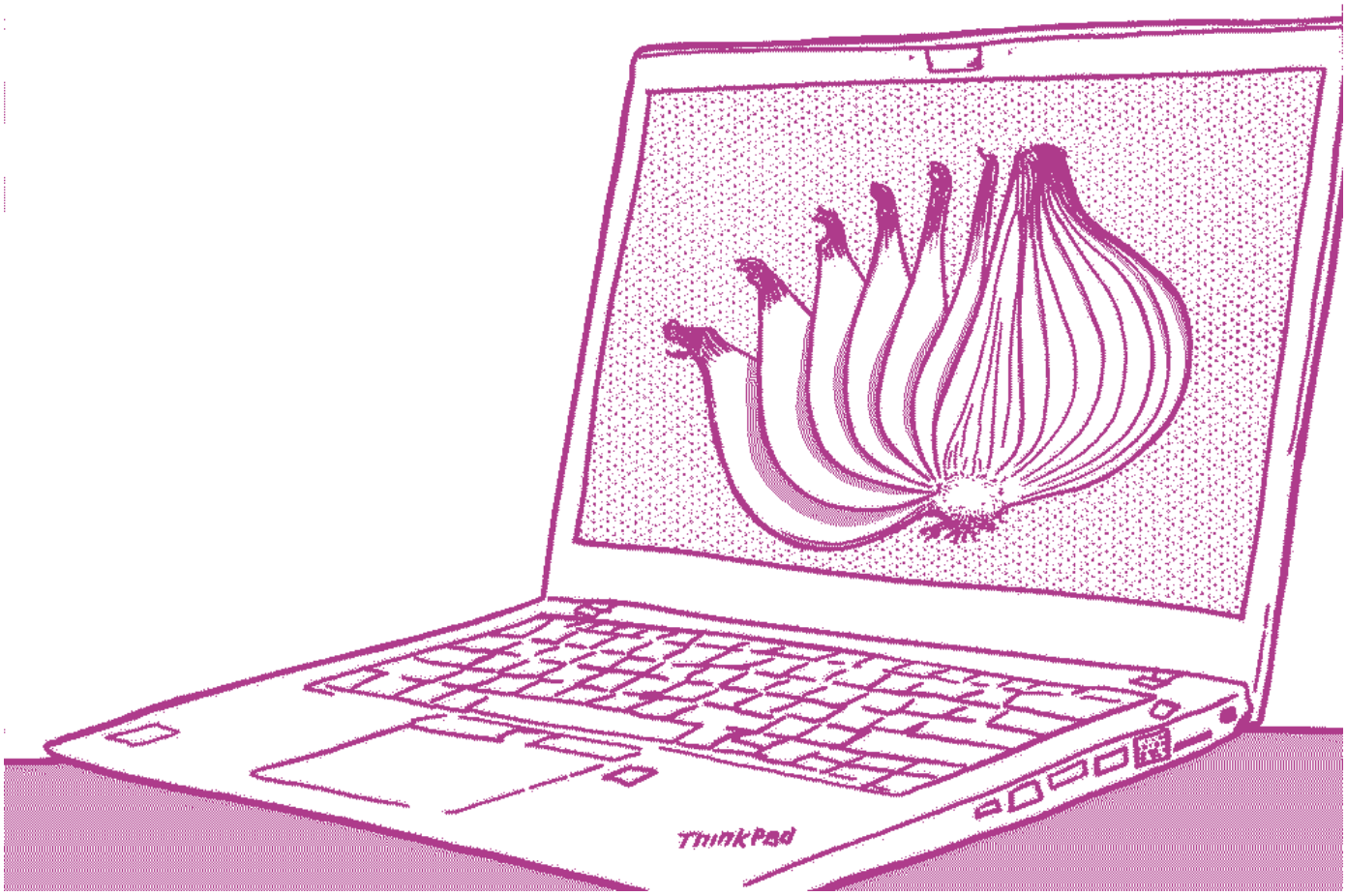
Tails for Anarchists



Serie: Difensiva

Questa è la traduzione in italiano di un opuscolo che è stato aggiornato l'ultima volta il 26.04.2024, per cui alcune più recenti versioni di Tails differiscono leggermente da come qui descritte. Tenete d'occhio il sito https://www.anarsec.guide/posts/tails/ [in inglese] per avere ulteriori aggiornamenti.
L'intento è quello di fomentare un utilizzo consapevole dei dispositivi elettronici che quotidianamente adoperiamo, in particolare quando li usiamo per scopi sovversivi. Non dimentichiamoci, però, che non esiste un uso del tutto sicuro della tecnologia; ciò non toglie che possiamo fare del nostro meglio per mitigarne i rischi.

Leggi, traduci, approfondisci e contribuisci anche tu a diffondere pratiche di sicurezza informatica: è importante sia per tutelare te stesso/a che le tue compagne/i!

Per consultare ulteriori manuali rivolti al giro anarchico (come questo): https://www.anarsec.guide (in inglese)

Il simbolo del pugnale † dopo una parola significa che vi è una voce corrispondente nel glossario in appendice. Ai ferri corti.

Indice

Tails è un sistema operativo† che rende l'uso anonimo del computer accessibile a tutt*. Tails è progettato[1] per non lasciare alcuna traccia delle tue attività sul computer, a meno che tu non lo configuri esplicitamente per salvare determinati dati. Ciò è possibile grazie all'esecuzione da DVD o USB, indipendentemente dal sistema operativo installato sul computer. Tails include diverse applicazioni integrate[2] preconfigurate con un occhio di riguardo alla sicurezza, e tutt* l* anarchic* dovrebbero sapere come utilizzarlo per comunicare, ricercare, modificare e pubblicare contenuti sensibili in modo sicuro.

La documentazione sul sito web di Tails[3] è eccellente e di facile consultazione. Questo tutorial riassume la documentazione più rilevante e fornisce consigli specifici per la configurazione e l'utilizzo di Tails in un contesto anarchico. Il nostro articolo sulle “Migliori pratiche” di Tails fornisce ulteriori dettagli, ma ti consigliamo di familiarizzare con i concetti base di Tails prima di leggerlo.

TAILS: Il sistema operativo live Amnesia e Incognito

Tails è un sistema operativo. Un sistema operativo è l'insieme di programmi che gestiscono i vari componenti (disco rigido, schermo, processore, memoria, ecc.) del computer e ne consentono il funzionamento.

Probabilmente avrete sentito parlare di "Windows" o "macOS", i due sistemi operativi più diffusi. Esistono però anche altri sistemi operativi: hai mai sentito parlare di Linux? Linux è una famiglia di sistemi operativi che si ramifica in diverse sottofamiglie, o versioni, una delle quali è Debian. Nella sottofamiglia Debian troviamo Ubuntu e Tails. Tails è una distribuzione di Linux con diverse caratteristiche distintive:

- ***Sistema live***

Tails è un sistema operativo live. A differenza degli altri sistemi operativi, che vengono eseguiti dal disco rigido del computer, Tails viene installato su un dispositivo esterno, come una chiavetta USB (o anche una scheda SD o un DVD). Quando si avvia il computer con il dispositivo Tails collegato, il sistema operativo viene eseguito da quel dispositivo senza lasciare traccia sul disco rigido. È possibile utilizzare Tails anche su un computer sprovvisto di disco rigido.

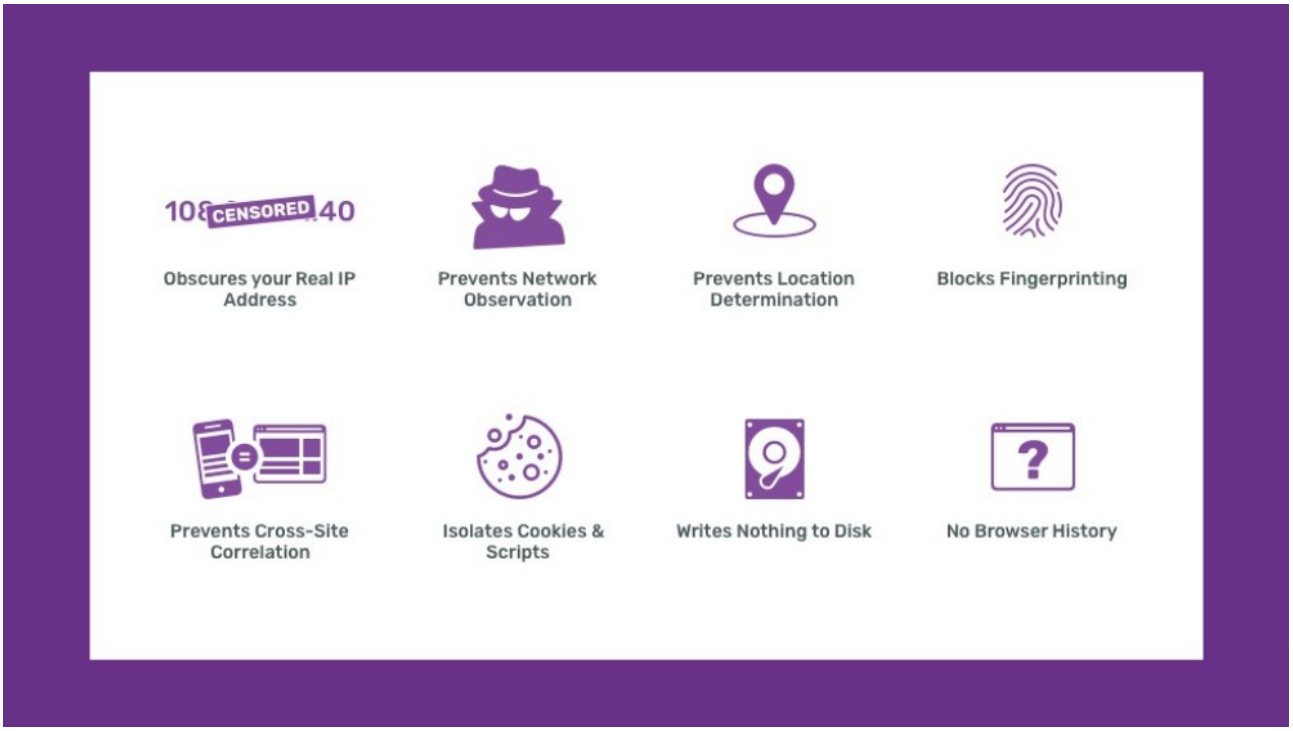
- ***Amnesia***

Tails è progettato per non lasciare alcuna traccia sul computer in uso: non scrive nulla sul disco rigido e funziona solo nella RAM (memoria), che viene automaticamente cancellata allo spegnimento. Anche il sistema live di Tails (che di solito funziona su una chiavetta USB) rimane intatto. L'unico modo per salvare le informazioni è spostarle su un'altra partizione USB prima dello spegnimento (vedere sotto). L'obiettivo è evitare di lasciare tracce forensi che qualcuno con accesso fisico al computer o alla chiavetta USB di Tails potrebbe leggere in un secondo momento. Cose come la cronologia delle ricerche su Internet, i documenti "modificati di recente", ecc. vengono tutte cancellate.

1 tails.net/about/index.en.html
2 tails.net/doc/about/features/index.en.html
3 tails.net/doc/index.en.html

- ***Incognito***

Tails è anche un sistema che consente di navigare in incognito, ovvero in modo anonimo. Nasconde gli elementi che potrebbero rivelare la tua identità, la tua posizione, ecc. Tails utilizza la rete anonima Tor† per proteggere il tuo anonimato online, costringendo tutti i software predefiniti a connettersi a Internet tramite Tor. Se un'applicazione tenta di connettersi direttamente a Internet, Tails bloccherà automaticamente la connessione. Tails modifica anche l'indirizzo MAC dell'hardware di rete, che può essere utilizzato per identificare in modo univoco il tuo laptop.



- ***Sicurezza***

Tails è stato progettato pensando alla sicurezza. È già installato un ambiente minimale, funzionale e verificato, con tutto il necessario per l'elaborazione di testi di base, l'editing di immagini, la crittografia†, ecc.

La sicurezza digitale di oggi non è necessariamente quella di domani. **La protezione dei dati personali richiede aggiornamenti regolari.** Gli strumenti digitali non sono affidabili se non vengono mai aggiornati e, per poter riporre fiducia duratura in questi strumenti, è importante sapere che i team che li sviluppano li mantengono attivamente e che godono di buona reputazione. È importante comprendere lo spirito di Tails: tutto è progettato pensando alla sicurezza. Tuttavia, nel campo del software non esistono strumenti perfetti e ci sono sempre dei limiti. Inoltre, **l'uso che si fa di Tails può creare problemi di sicurezza**.

Tails è un software gratuito e *open source*†. Chiunque può visualizzare, scaricare e modificare il codice sorgente (la ricetta). È assolutamente necessario assicurarsi che la versione di Tails in uso sia autentica. Non trascurate le fasi di verifica durante l'installazione, ben spiegate sul sito web di Tails.

Tails permette anche agli utenti meno esperti di beneficiare della sicurezza digitale e dell'anonimato senza dover affrontare una curva di apprendimento ripida. L'uso di Tor† è fondamentale per garantire l'anonimato digitale e Tails ci aiuta a commettere il minor numero possibile di errori durante l'utilizzo di

Tor e di altri strumenti simili. L'uso di Tails richiede uno sforzo minimo per rendere più sicuro il comportamento digitale quotidiano, anche se a volte può sembrare "scomodo". L'alternativa "comoda", d'altra parte, comporta un aumento del rischio di repressione, non solo per te, ma anche per le persone con cui comunichi.

Questo tutorial è suddiviso in diverse sezioni. La prima sezione tratta le nozioni di base per iniziare a utilizzare Tails. La seconda sezione fornisce suggerimenti sull'uso delle applicazioni incluse in Tails e informazioni utili sul funzionamento di Tor. La terza sezione è dedicata alla risoluzione dei problemi che potresti incontrare con la tua chiavetta USB Tails: non arrenderti al primo intoppo, perché nella maggior parte dei casi la soluzione è semplice!

Il concetto di Threat Model [modello di rischio]

Tails non è magico e presenta molti limiti. Internet e i computer sono un territorio ostile, progettato per rubare i tuoi dati. Tails non ti proteggerà dagli errori umani, dall'hardware o dal firmware compromesso, dagli hacker o da altri tipi di attacco. Non esiste una sicurezza perfetta su Internet, motivo per cui è così importante costruire un "modello di rischio"†.

Costruire un modello di rischio significa semplicemente porsi alcune domande. Da chi mi sto difendendo? Quali sono le loro capacità? Quali sarebbero le conseguenze se avessero accesso a quei dati? Poi, in base alla situazione specifica, si deve valutare come proteggersi.

Non ha senso dire: "Questo strumento è sicuro". La sicurezza dipende sempre dal modello di rischio e si articola su più livelli (rete, hardware, software, ecc.). Per ulteriori informazioni su questo argomento, consultare la Threat Library[4].

I) Nozioni di base sull'uso di Tails

Prerequisiti

Scegliere una chiavetta USB/un DVD:

Tails funziona solo con chiavette USB da almeno 8 GB, DVD o schede SD. Durante l'installazione, tutti i dati presenti sulla USB verranno cancellati, quindi è necessario salvarli altrove prima di procedere. Se non si desidera lasciare alcuna traccia di ciò che era presente in precedenza, è consigliabile utilizzare una nuova USB.

L'articolo sulle “Migliori pratiche” di Tails consiglia di utilizzare una chiavetta USB con un interruttore di protezione da scrittura (un disco non modificabile). Quando è bloccato, l'interruttore impedisce qualsiasi modifica al contenuto della chiavetta USB. Ciò impedisce che una sessione Tails compromessa possa compromettere la tua USB Tails. L'interruttore di protezione da scrittura (in inglese, *write-protect switch*) deve essere disattivato durante l'installazione. Se non si riesce a procurarsi una USB di questo tipo, è possibile eseguire Tails da una scheda SD o DVD-R/DVD+R oppure avviare sempre con l'opzione `toram` (descritta nell'articolo).

4 notrace.how/threat-library/

Scegliere un laptop:

Sebbene sia possibile utilizzare Tails su un computer fisso, non è consigliabile, in quanto è possibile rilevare eventuali manomissioni fisiche solo su un laptop. Per ulteriori informazioni su come procurarti un laptop, consulta la sezione “Migliori Pratiche” di Tails in quest’opuscolo.

Alcuni modelli di laptop e di chiavette USB non sono compatibili con Tails o non supportano tutte le funzionalità. Per verificare se il tuo modello presenta problemi noti, consulta la pagina dei problemi noti di Tails[5].

Se Tails è troppo lento, assicurati che la tua chiavetta USB sia 3.0 o superiore e che tu stia utilizzando una porta USB 3.0 sul laptop. Se Tails si blocca frequentemente, puoi aggiungere più RAM al tuo computer. 8 GB dovrebbero essere sufficienti.

Installazione

Per installare Tails su una USB, hai bisogno di una “fonte” e di una USB (da 8 GB o superiore).

Ci sono due soluzioni per la "fonte":

Soluzione 1: installazione tramite download (preferibile)

Segui le istruzioni di installazione di Tails, è importante seguire l'intero tutorial. È possibile che un malintenzionato intercetti e modifichi i dati mentre ti vengono inviati (si tratta di un attacco *man-in-the-middle†*), quindi non saltare i passaggi di verifica. Come discusso nelle “Migliori Pratiche” di Tails, il metodo di installazione GnuPG† è preferibile, in quanto verifica in modo più approfondito l'integrità del download.

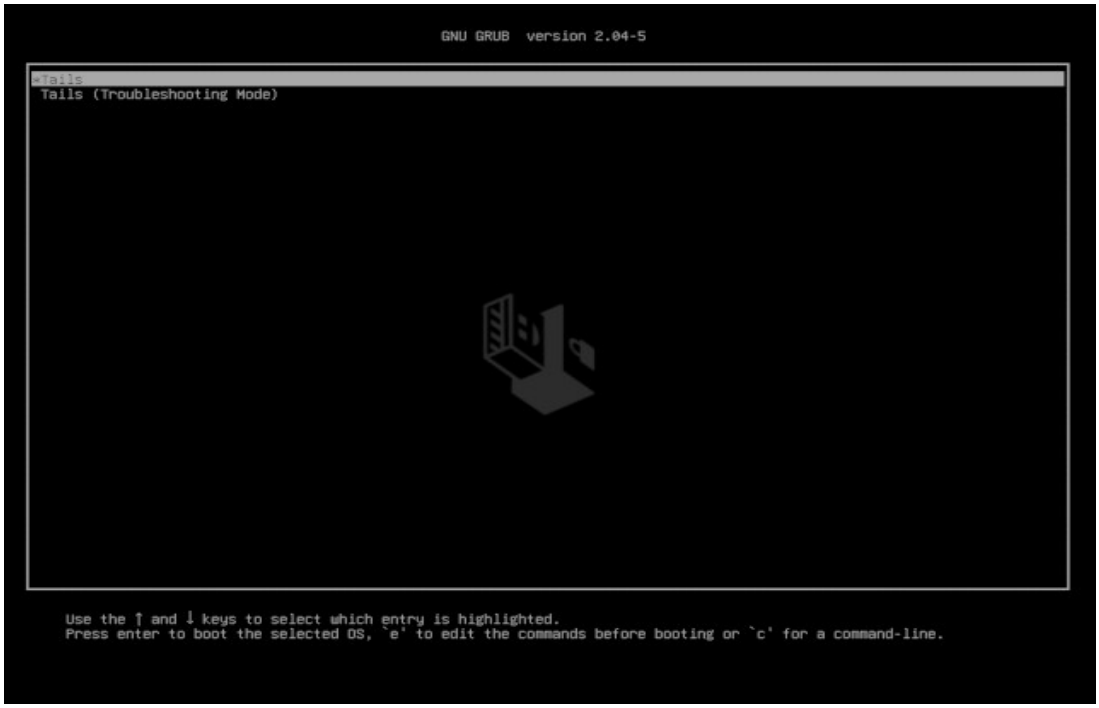
Soluzione 2: installazione da un'altra USB Tails

Questo metodo richiede di conoscere un utente Tails di cui ti fidi. Un software molto semplice chiamato Tails Installer ti consente di "clonare" una chiavetta USB Tails esistente su una nuova in pochi minuti; consulta la documentazione per la clonazione da PC o Mac sul sito di Tails. I dati della memoria permanente non verranno trasferiti. Lo svantaggio di questo metodo è che potrebbe diffondere un'installazione compromessa.

Avvio [*boot*] da USB Tails

Una volta ottenuta una USB Tails, segui le istruzioni di Tails per avviarlo su un Mac o un PC. L'USB Tails deve essere inserita prima di accendere il laptop. Si aprirà la schermata Boot Loader e Tails si avvierà automaticamente dopo alcuni secondi.

5 tails.net/support/known_issues/



Dopo circa 30 secondi di caricamento, apparirà la schermata di benvenuto.

Nella schermata di benvenuto, seleziona la lingua e il layout della tastiera nella sezione "**Lingua e regione**". Per gli utenti Mac, è disponibile un layout della tastiera per Macintosh. Sotto "Impostazioni aggiuntive" troverai un pulsante +: cliccandolo, appariranno ulteriori opzioni di configurazione.

- **Password di amministrazione**

Impostala se hai bisogno dei diritti di amministrazione. Ciò è necessario, ad esempio, per installare software aggiuntivi che desideri utilizzare durante la tua sessione Tails. Nella finestra di dialogo seguente, puoi inserire qualsiasi password (e ricordarla!). Sarà valida solo per questa sessione di Tails.

Una volta terminata l'attività che richiedeva l'accesso con la password di amministrazione, riavvia la sessione Tails senza password.

- **Spoofing dell'indirizzo MAC**

Si consiglia di non disabilitare mai questa opzione. È abilitata per impostazione predefinita.

- **Connessione di rete**

“Disabilita tutte le reti" consente di disabilitare tutti gli adattatori di rete software all'avvio. Se si desidera avere una sessione Tails "offline", è opportuno farlo prima che Tails avvii la sua funzionalità di rete.

- **Browser non sicuro**

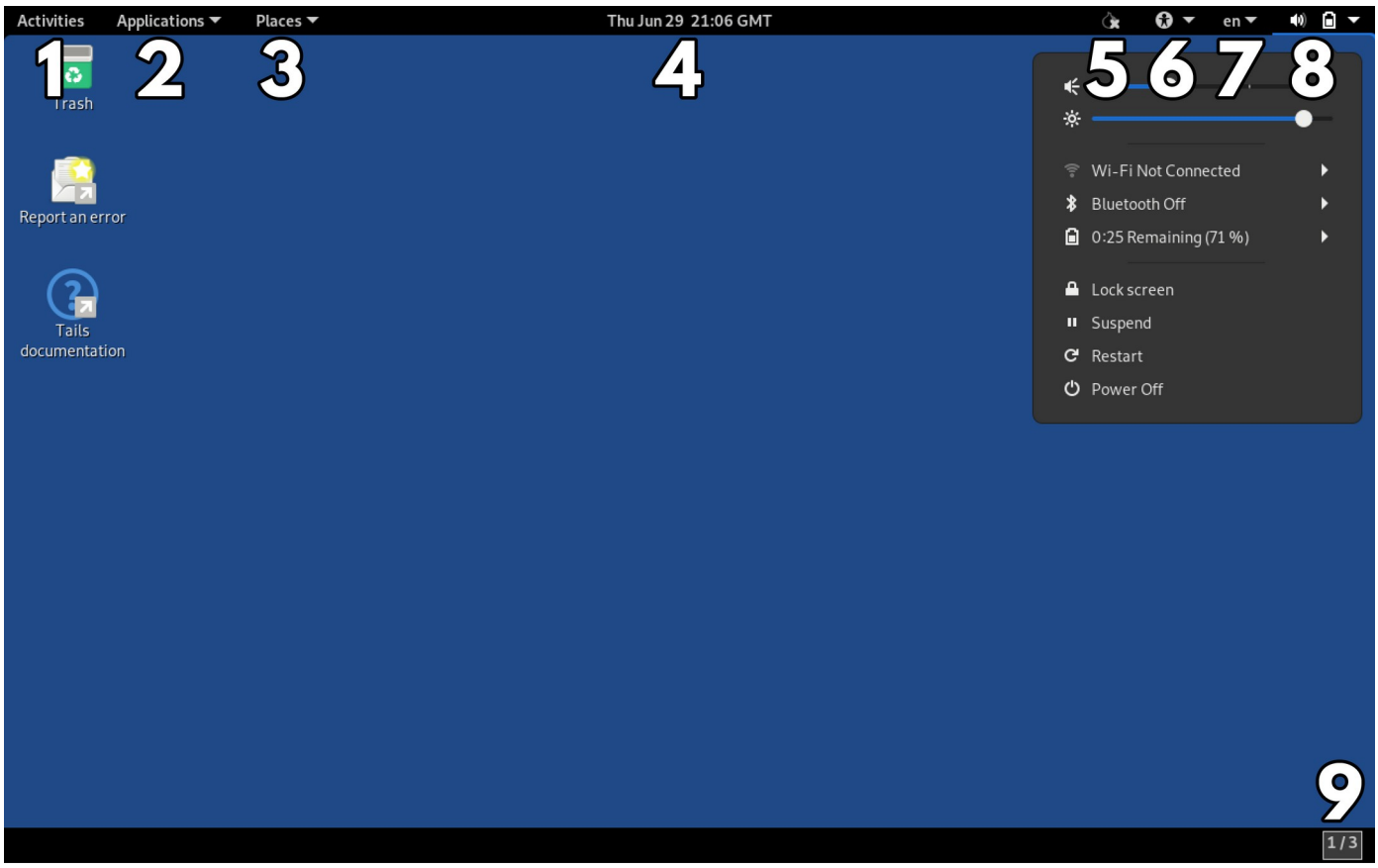
“Browser non sicuro” è abilitato per impostazione predefinita e non utilizza Tor. Un malintenzionato potrebbe usare un exploit† tramite una vulnerabilità† in un'altra applicazione di Tails per avviare un “Browser non sicuro” invisibile e rivelare il tuo indirizzo IP reale. Ciò è possibile anche se non si sta utilizzando il browser non sicuro. Per esempio, un malintenzionato potrebbe sfruttare una vulnerabilità in Thunderbird inviandoti un'e-mail di *phishing*† che avvia un “Browser non sicuro” invisibile che visita un sito web e rivela il tuo indirizzo IP. Un attacco di questo tipo è molto improbabile, ma potrebbe essere messo in atto da un aggressore potente, come un governo o un'azienda di hacking. Per questo motivo, ti **consigliamo di disattivare Browser non sicuro per ogni sessione**. Lascia il “Browser non sicuro” abilitato solo quando devi passare attraverso un "*captive portal*" per connetterti a Internet (quando devi cliccare su una casella o effettuare il login per connetterti a Internet, cosa comune negli internet café, nelle reti Wi-Fi pubbliche, ecc.).

Se hai abilitato Archiviazione Persistente, la passphrase per sbloccarlo apparirà in questa finestra. Se non hai abilitato Archiviazione Persistente, nessun dato verrà memorizzato sulla tua USB Tails oltre questa sessione. Clicca su "**Avvia Tails**". Dopo 15-30 secondi, apparirà il desktop di Tails.Nella schermata di benvenuto, seleziona la lingua e il layout della tastiera nella sezione "**Lingua e regione**". Per gli utenti Mac, è disponibile un layout della tastiera per Macintosh. Sotto "Impostazioni aggiuntive" troverai un pulsante +: cliccandolo, appariranno ulteriori opzioni di configurazione.

- **Password di amministrazione.**

Impostala se hai bisogno dei diritti di amministrazione. Ciò è necessario, ad esempio, per installare software aggiuntivi che desideri utilizzare durante la tua sessione Tails. Nella finestra di dialogo seguente, puoi inserire qualsiasi password (e ricordarla!). Sarà valida solo per questa sessione di Tails. Una volta terminata l'attività che richiedeva l'accesso con la password di amministrazione, riavvia la sessione Tails senza password.

Utilizzo del desktop di Tails



Tails è un sistema operativo semplice.

1. Il menu Attività. Consente di visualizzare una panoramica delle finestre e delle applicazioni. Consente inoltre di cercare applicazioni, file e cartelle. È possibile accedere alle Attività anche spostando il mouse nell'angolo in alto a sinistra dello schermo o premendo il tasto Comando/Windows (❖).
2. Il menu Applicazioni. Elenca le applicazioni disponibili (software), organizzate per categoria.
3. Il menu Luoghi. - Collegamenti a varie cartelle e dispositivi di archiviazione, accessibili anche tramite il browser File (**Applicazioni** > **Accessori** > **File**).
4. Data e ora. Una volta connessi a Internet, tutti i sistemi Tails nel mondo condividono la stessa ora.
5. L'indicatore di stato di Tor. Indica se sei conness* alla rete Tor. Se sull'icona a forma di cipolla è presente una X, significa che non sei conness*. Da qui puoi aprire l'applicazione Onion Circuits. Per verificare la tua connessione Tor, visita `check.torproject.org` nel browser Tor.
6. Il pulsante "Accesso universale". Questo menu ti consente di abilitare software di accessibilità come lo screen reader, la tastiera visiva e la visualizzazione del testo ingrandito.
7. Scelta dei layout di tastiera. Un'icona che mostra il layout della tastiera corrente (nell'esempio sopra, "en" per un layout inglese). Cliccando su di essa, si ottengono le opzioni per altri layout selezionati nella schermata di benvenuto.
8. Il menu "Sistema". Da qui è possibile accedere al volume e alla luminosità dello schermo, alla connessione Wi-Fi e a quella Ethernet, allo stato della batteria e ai pulsanti di riavvio e spegnimento.
9. L'icona Spazi di lavoro. Questo pulsante consente di passare da una visualizzazione all'altra del desktop (chiamate "*workspaces*"), il che può aiutare a ridurre l'ingombro visivo su uno schermo piccolo.

Se il tuo laptop è dotato di Wi-Fi, ma nel menu di sistema non è presente l'opzione Wi-Fi, consulta la documentazione relativa alla risoluzione dei problemi. Una volta connesso al Wi-Fi, apparirà un assistente di connessione a Tor che ti guiderà nella connessione alla rete Tor. Seleziona "**Connetti automaticamente a Tor**", a meno che tu non ti trovi in un Paese in cui è necessario nascondere l'utilizzo di Tor (in tal caso, dovrai configurare un bridge).

Facoltativo: creare e configurare l'archiviazione persistente

Tails è amnesico per impostazione predefinita. Dimenticherà tutto ciò che hai fatto non appena terminerai la sessione. Tuttavia, questo non è sempre ciò che si desidera: ad esempio, potresti voler installare software aggiuntivo senza doverlo reinstallare ogni volta che si avvia il sistema. Tails dispone di una funzione chiamata "Archivio persistente" che ti permette di salvare i dati tra una sessione e l'altra. Questa funzione è meno sicura, ma necessaria per alcune attività.

Il principio alla base dell'archiviazione persistente è quello di creare una seconda area di archiviazione (chiamata "partizione") sulla tua chiavetta USB Tails, che è crittografata. Questa nuova partizione ti permette di rendere persistenti alcuni dati, ovvero di conservarli tra una sessione e l'altra di Tails. Abilitare l'archiviazione persistente è molto semplice. Per creare l'archiviazione persistente, seleziona **Applicazioni > Tails > Archiviazione persistente**.

Si aprirà una finestra che ti chiederà di inserire una *passphrase*; consulta la sezione “Migliori pratiche di Tails” per informazioni sulla sicurezza delle *passphrase*. A questo punto, sarà possibile configurare i dati da conservare nell'archiviazione persistente. L'archiviazione persistente può essere abilitata per diversi tipi di dati:

Documenti personali:

- **Cartella persistente:** dati quali file personali, documenti o immagini su cui si sta lavorando.

Impostazioni di sistema:

- **Schermata di benvenuto**: impostazioni della schermata di benvenuto (lingua, tastiera e impostazioni aggiuntive);
- **Stampanti**: configurazione della stampante.

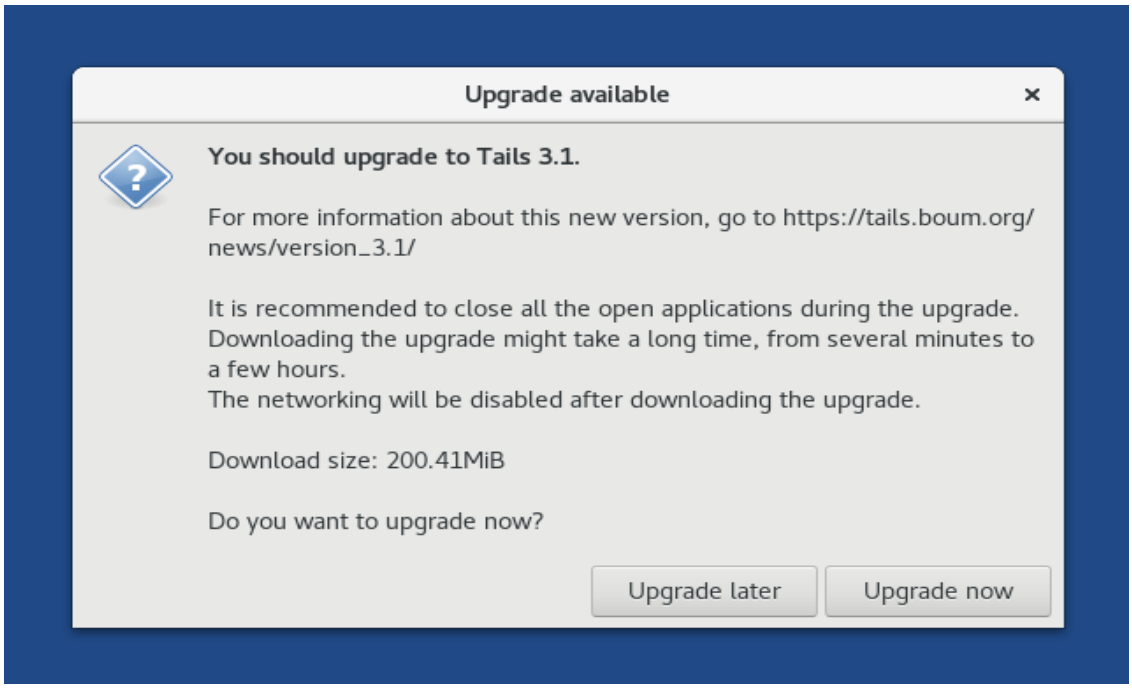
Rete:

- **Connessioni di rete:** le password delle reti Wi-Fi possono essere salvate in modo da non doverle inserire ogni volta.
- **Tor Bridge**: se Tor Bridge è abilitato (per gli utenti nei paesi che censurano Tor), verrà memorizzato l'ultimo Tor Bridge utilizzato.

Applicazioni:

- **Tor Browser bookmarks:** i segnalibri Tor Browser.
- **Electrum Bitcoin Wallet:** il portafoglio Bitcoin e le relative impostazioni.

- **Client di posta elettronica Thunderbird:** la casella di posta elettronica Thunderbird, i feed e le chiavi OpenPGP.
- **GnuPG†:** le chiavi OpenPGP create o importate in GnuPG e Kleopatra.
- **Pidgin:** i file dell'account di questa applicazione di chat (che utilizza il protocollo XMPP).
- **Client SSH:** tutti i file relativi a SSH, un protocollo utilizzato per connettersi ai server.



Impostazioni avanzate:

- **Software aggiuntivo:** se questa funzione è abilitata, ogni volta che avvii Tails verrà installato automaticamente un elenco di software aggiuntivo di tua scelta. Questi pacchetti software sono memorizzati nella memoria permanente. Vengono aggiornati automaticamente quando ti connetti a Internet. Fai attenzione a ciò che installi.
- **File dot:** in Tails e in Linux in generale, i nomi dei file di configurazione spesso iniziano con un punto, quindi a volte vengono chiamati “file dot”. Questi possono essere salvati nella memoria persistente. Fai attenzione alle impostazioni di configurazione che modifichi, poiché la modifica delle impostazioni predefinite può compromettere il tuo anonimato.

Per utilizzare l’Archivio Persistente (*Persistent Storage*), è necessario sbloccarlo dalla schermata di benvenuto. Se si desidera modificare la *passphrase*, consultare la documentazione. Se la si dimentica, non è possibile recuperarla e sarà necessario eliminare la Persistenza e ricominciare da capo.

Nella sezione “Migliori pratiche” di Tails, sconsigliamo l'uso della memoria persistente nella maggior parte dei casi: la maggior parte delle sue funzioni non è compatibile con le chiavette USB dotate di interruttore di protezione da scrittura e qualsiasi file memorizzato su una chiavetta USB Tails lascia tracce forensi su di essa. Inoltre, la memorizzazione di dati personali sulla chiavetta USB Tails impedisce la compartimentazione quando la memoria persistente è sbloccata. Qualsiasi file che deve essere persistente può essere memorizzato su una seconda chiavetta USB crittografata con LUKS†.

Aggiornamento della USB Tails

Per garantire la sicurezza di Tails, il sistema operativo deve essere costantemente aggiornato e qualsiasi vulnerabilità† deve essere risolta tramite aggiornamenti. È importante utilizzare sempre l'ultima versione (Tails viene aggiornato circa ogni mese), perché nei programmi utilizzati da Tails vengono regolarmente scoperte falle di sicurezza che, nel peggiore dei casi, potrebbero portare alla divulgazione della tua identità, del tuo indirizzo IP, ecc. Un aggiornamento di Tails risolverà queste vulnerabilità e di solito migliorerà anche altre funzionalità.

Ogni volta che si avvia Tails, subito dopo la connessione alla rete Tor, Tails Upgrader verifica se si dispone dell'ultima versione di Tails. Esistono due tipi di aggiornamenti:

L'aggiornamento automatico

Quando è disponibile un aggiornamento automatico, viene visualizzata una finestra con le informazioni relative all'aggiornamento e bisogna cliccare su "**Aggiorna ora**" [*Upgrade now*]. Attendere qualche istante affinché l'aggiornamento venga completato, quindi fare clic su "Applica aggiornamento" e la connessione a Internet verrà interrotta per un momento. Attendere fino a quando non viene visualizzata la finestra "Riavvia Tails". Se l'aggiornamento non va a buon fine (ad esempio, se spegni il computer prima che sia completato), la tua memoria persistente non verrà compromessa, ma potresti non riuscire a riavviare la tua USB Tails. Se la tua USB dispone di un interruttore di protezione da scrittura, dovrai sbloccarlo per la sessione dedicata in cui stai eseguendo l'aggiornamento.

L'aggiornamento manuale

A volte, la finestra di aggiornamento ti indicherà che è necessario eseguire un aggiornamento manuale. Questo tipo di aggiornamento viene utilizzato solo per gli aggiornamenti importanti (che avvengono circa ogni due anni) o in caso di problemi con gli aggiornamenti automatici. Consulta la documentazione sugli aggiornamenti manuali[6].

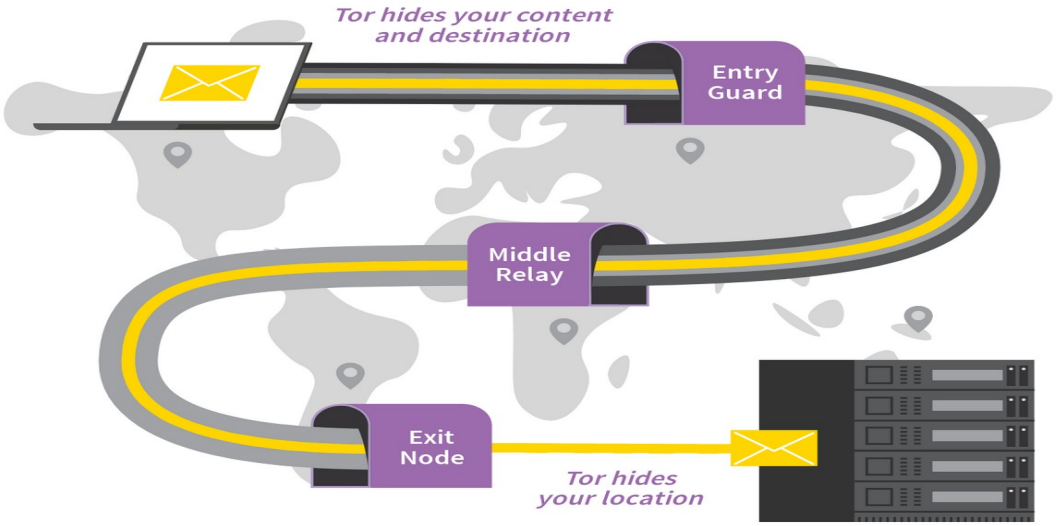
II) Approfondimenti: alcuni suggerimenti e spiegazioni

Tor

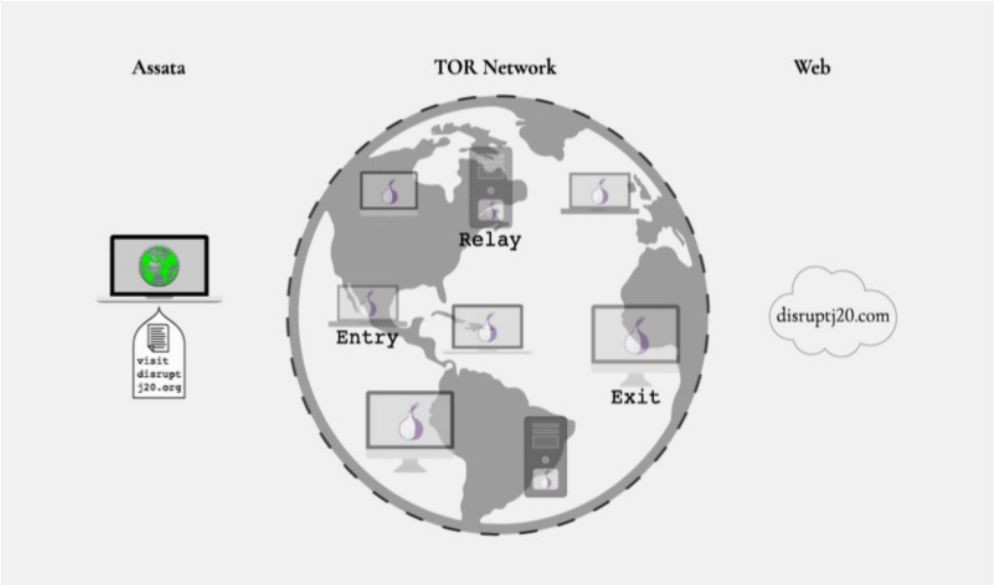
Che cos'è Tor?

Tor†, acronimo di The Onion Router, è il modo migliore per navigare in modo anonimo su Internet. Tor è un software open source collegato a una rete pubblica di migliaia di relay (server). Invece di connettersi direttamente a una posizione su Internet, Tor effettua una deviazione attraverso tre relay intermedi. Il browser Tor utilizza la rete Tor, ma anche altre applicazioni possono farlo, a condizione che siano configurate correttamente. Tutte le applicazioni predefinite incluse in Tails utilizzano Tor quando devono connettersi a Internet.

6 Tails.net/upgrade/tails/index.en.html



Il traffico Internet, compreso l'indirizzo IP della destinazione finale, viene crittografato a strati, come una cipolla. Ogni relay rimuove uno strato di crittografia†. Ogni relay conosce solo il relay che lo precede e quello che lo segue (il relay di uscita sa che proviene dal relay centrale e che è diretto a un determinato sito web, ma non conosce il relay di ingresso).



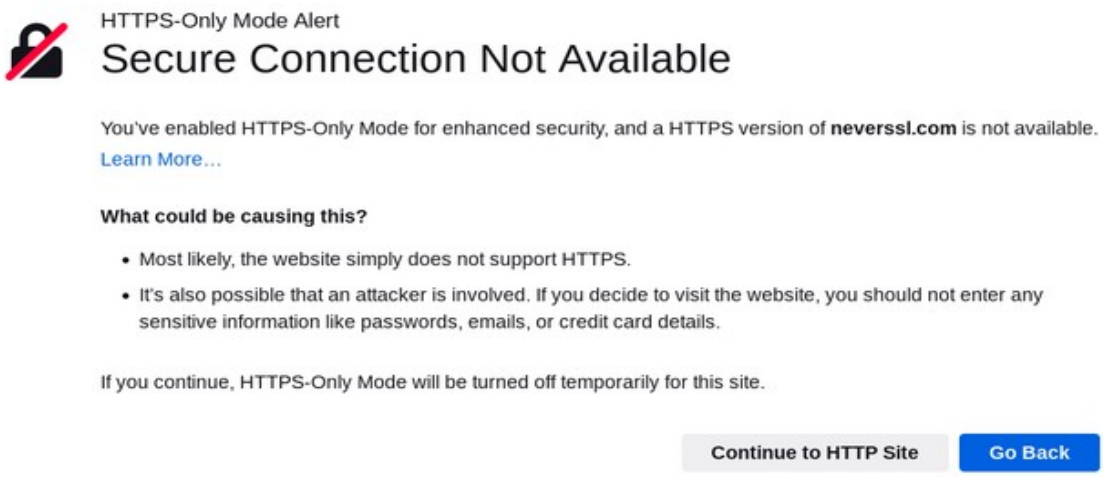
Ciò significa che qualsiasi intermediario tra te e il relay di ingresso sa che stai utilizzando Tor, ma non conosce il sito a cui stai accedendo. Qualsiasi intermediario dopo il relay di uscita sa che qualcuno nel mondo sta andando a quel sito, ma non sa chi sia. Il server web del sito vede che provieni dall'indirizzo IP del relay di uscita.

Tor presenta diverse limitazioni. Ad esempio, se qualcuno con i mezzi tecnici e legali ritiene che ti stia connettendo da una determinata connessione Wi-Fi per visitare un sito specifico, può provare a correlare la tua connessione Wi-Fi all'attività del sito web (un "attacco di correlazione"). Tuttavia, per quanto ne sappiamo, questo tipo di attacco non è mai stato utilizzato da solo per incriminare qualcuno in tribunale. Per attività sensibili, utilizza connessioni Internet che non siano riconducibili alla tua identità, così da proteggerti nel caso in cui Tor dovesse fallire.

Che cos'è HTTPS?

Praticamente tutti i siti web oggi utilizzano HTTPS†: la "S" sta per "sicuro" (ad esempio, `https://www.anarsec.guide`). Se provi a visitare un sito web senza "https://" nel browser Tor, riceverai un avviso prima di procedere. Se invece di `https://` vedi `http://` davanti all'indirizzo di un sito web, significa che tutti gli intermediari dopo il relay di uscita della rete Tor sanno cosa stai scambiando con il sito web (comprese le tue credenziali). HTTPS significa che la registrazione digitale delle tue attività sul sito che stai visitando è protetta da una chiave di crittografia† che appartiene al sito stesso. Gli intermediari dopo il relay di uscita sapranno che stai visitando, per esempio, riseup.net, ma non avranno accesso alle tue e-mail e alla tua password, né sapranno se stai controllando la tua casella di posta o leggendo una pagina casuale del sito. Quando si utilizza HTTPS, a sinistra dell'indirizzo del sito appare un piccolo lucchetto.

Se sul lucchetto compare un avviso giallo, significa che alcuni elementi della pagina che stai visualizzando non sono crittografati (utilizzano HTTP), il che potrebbe rivelare la pagina esatta o consentire agli intermediari di modificarla parzialmente. Per impostazione predefinita, il browser Tor utilizza la modalità HTTPS solo per impedire agli utenti di visitare siti HTTP.



HTTPS è essenziale sia per limitare la tua impronta digitale sul Web, sia per impedire a un intermediario di modificare i dati che scambi con i siti web. Se l'intermediario non può decifrare i dati, non può modificarli.

In breve, non visitare siti web che non utilizzano HTTPS.

Servizi Onion: cos'è .onion?

Hai mai visto un indirizzo web strano, con 56 caratteri casuali e il suffisso .onion? Si tratta di un servizio Onion e l'unico modo per visitare un sito web con un indirizzo di questo tipo è utilizzare il browser Tor. I termini "deep web" e "dark web" sono stati resi popolari dai media per descrivere questi servizi onion.

Chiunque può creare un sito .onion. Ma perché dovrebbe farlo? Beh, la posizione del server è anonima, quindi le autorità non possono scoprire dove è ospitato il sito per chiuderlo. Quando si inviano dati a un sito .onion, si entra nei tre relay Tor del sito dopo il circuito Tor standard. Ci sono quindi 6 relay Tor tra noi e il sito: noi conosciamo i primi 3, il sito conosce gli ultimi 3 e ogni nodo Tor conosce solo il relay precedente e quello successivo. A differenza di un normale sito web HTTPS, tutto è crittografato da Tor da un'estremità all'altra.

Ciò significa che sia il client (il tuo laptop) che il server (dove risiede il sito) rimangono anonimi, mentre con un sito web normale solo il client lo è. Oltre a garantire maggiore anonimato al server, il sistema offre maggiore anonimato anche all'utente: non si esce mai dalla rete Tor, quindi non è possibile intercettare l'utente dopo il relay di uscita.

L'indirizzo del sito .onion è lungo perché include il certificato del sito. L'HTTPS non è necessario, la sicurezza dipende dalla conoscenza dell'indirizzo .onion del sito.

Alcuni siti offrono sia un URL classico che un indirizzo .onion. In tal caso, se il sito è stato configurato in tal senso, accanto all'URL dovrebbe apparire l'indicazione ".onion disponibile". In caso contrario, a volte l'indirizzo .onion è elencato da qualche parte nella pagina del sito. Per scoprire gli indirizzi dei siti disponibili solo come .onion, è necessario trovarli tramite passaparola o attraverso siti web che elencano altri siti .onion, come questa pagina GitHub[7].

Siti che bloccano Tor

Alcuni siti bloccano gli utenti che li visitano tramite la rete Tor o rendono la navigazione comunque scomoda. Alcuni siti potrebbero richiedere di completare dei CAPTCHA o di fornire ulteriori informazioni personali (come l'ID o il numero di telefono) prima di poter proseguire, oppure potrebbero bloccare completamente Tor.Chiunque può creare un sito .onion. Ma perché dovrebbe farlo? Beh, la posizione del server è anonima, quindi le autorità non possono scoprire dove è ospitato il sito per chiuderlo. Quando si inviano dati a un sito .onion, si entra nei tre relay Tor del sito dopo il circuito Tor

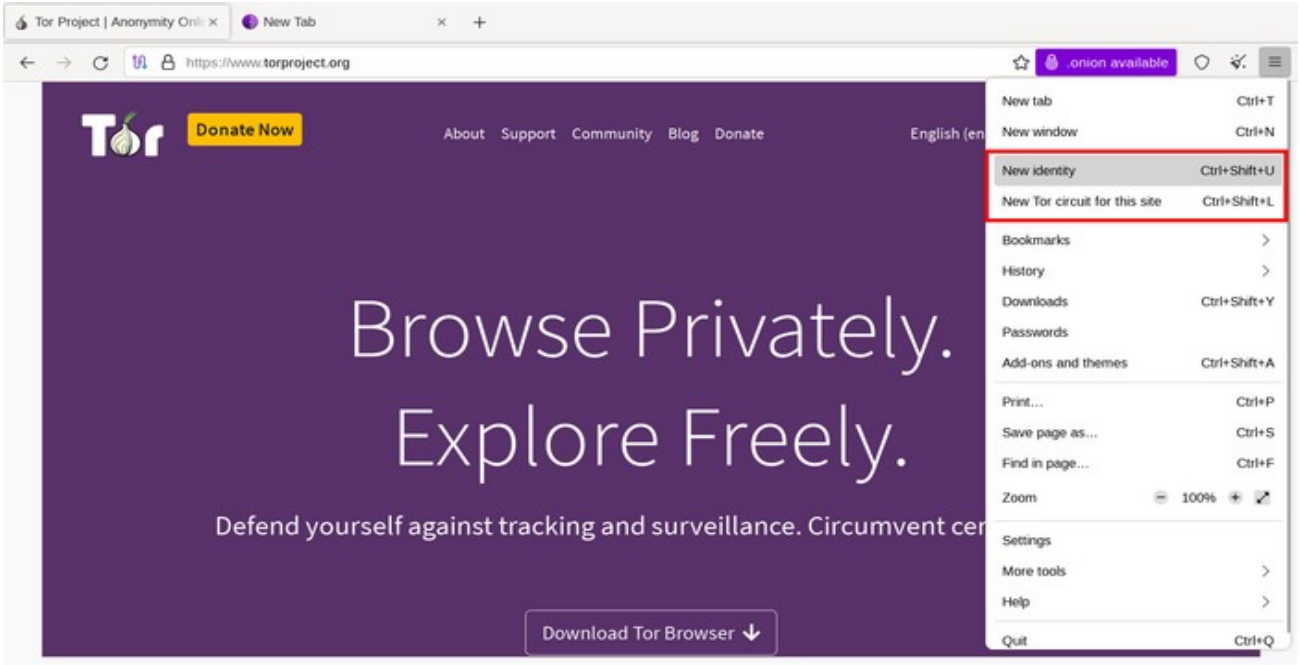
7 https://github.com/alecmuffett/real-world-onion-sites

standard. Ci sono quindi 6 relay Tor tra noi e il sito: noi conosciamo i primi 3, il sito conosce gli ultimi 3 e ogni nodo Tor conosce solo il relay precedente e quello successivo. A differenza di un normale sito web HTTPS, tutto è crittografato da Tor da un'estremità all'altra.

Ciò significa che sia il client (il tuo laptop) che il server (dove risiede il sito) rimangono anonimi, mentre con un sito web normale solo il client lo è. Oltre a garantire maggiore anonimato al server, il sistema offre maggiore anonimato anche all'utente: non si esce mai dalla rete Tor, quindi non è possibile intercettare l'utente dopo il relay di uscita.

L'indirizzo del sito .onion è lungo perché include il certificato del sito. L'HTTPS non è necessario, la sicurezza dipende dalla conoscenza dell'indirizzo .onion del sito.

Alcuni siti offrono sia un URL classico che un indirizzo .onion. In tal caso, se il sito è stato configurato in tal senso, accanto all'URL dovrebbe apparire l'indicazione ".onion disponibile". In caso contrario, a volte l'indirizzo .onion è elencato da qualche parte nella pagina del sito. Per scoprire gli indirizzi dei siti disponibili solo come .onion, è necessario trovarli tramite passaparola o attraverso siti web che elencano altri siti .onion, come questa pagina GitHub[8].



Il sito potrebbe bloccare solo alcuni relay Tor. In questo caso, è possibile cambiare il nodo di uscita Tor utilizzato per quel sito: fare clic sul pulsante ≣ e poi su "**Nuovo circuito Tor per questo sito**". Il circuito Tor (ovvero il percorso) cambierà per la scheda corrente e per tutte le altre schede o finestre aperte dello stesso sito web. Potrebbe essere necessario ripetere questa operazione più volte di seguito se si incontrano più relay vietati.

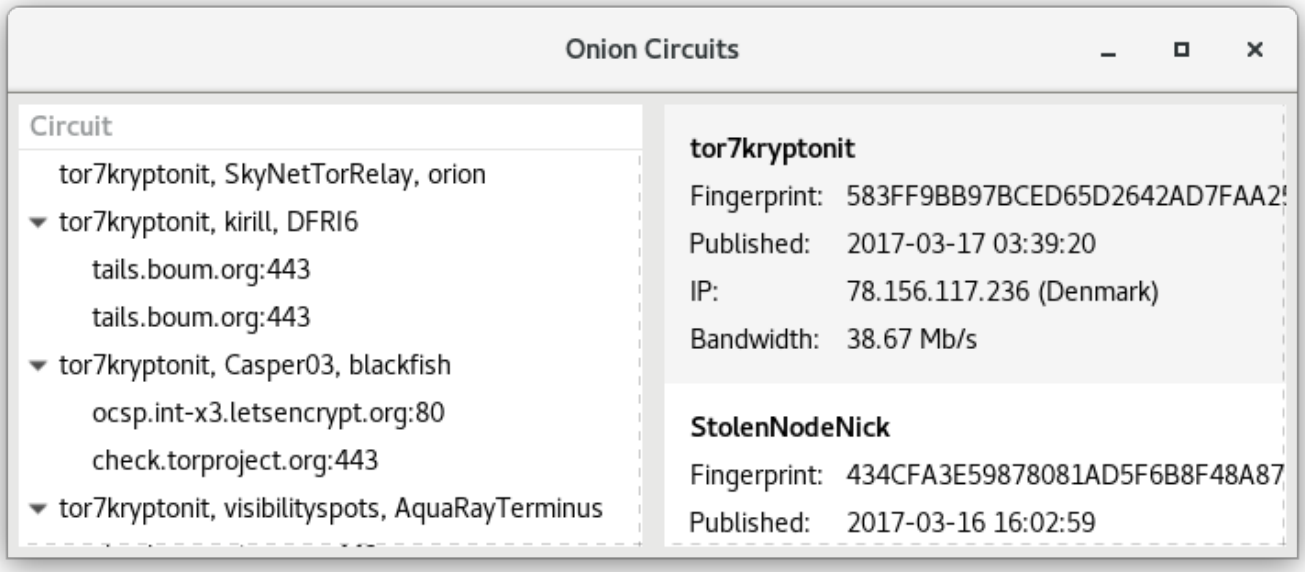
Poiché tutti i relay Tor sono pubblici, è anche possibile che il sito stia bloccando l'intera rete Tor. In tal caso, puoi provare a utilizzare un proxy per accedere al sito, come `https://hide.me/en/proxy` (ma solo se non devi inserire informazioni personali, come le credenziali di accesso). Puoi anche verificare se la pagina a cui desideri accedere è stata salvata su Wayback Machine: `web.archive.org`.

8 https://github.com/alecmuffett/real-world-onion-sites

Separare chiaramente le identità anonime

Non è consigliabile eseguire diverse attività su Internet che non dovrebbero essere associate tra loro durante la stessa sessione di Tails. È necessario separare attentamente le diverse identità (concomitanti)! Per esempio, è pericoloso controllare la propria posta elettronica personale e pubblicare un testo anonimo durante la stessa sessione. In altre parole, non si dovrebbe essere identificabili e anonimi sulla rete Tor allo stesso tempo. Non si dovrebbe nemmeno utilizzare la rete Tor con pseudonimi diversi nella stessa sessione, perché questi pseudonimi potrebbero essere collegati tramite un relay di uscita Tor monitorato o compromesso. È necessario chiudere e riavviare Tails tra un'attività Internet e l'altra con identità diverse!

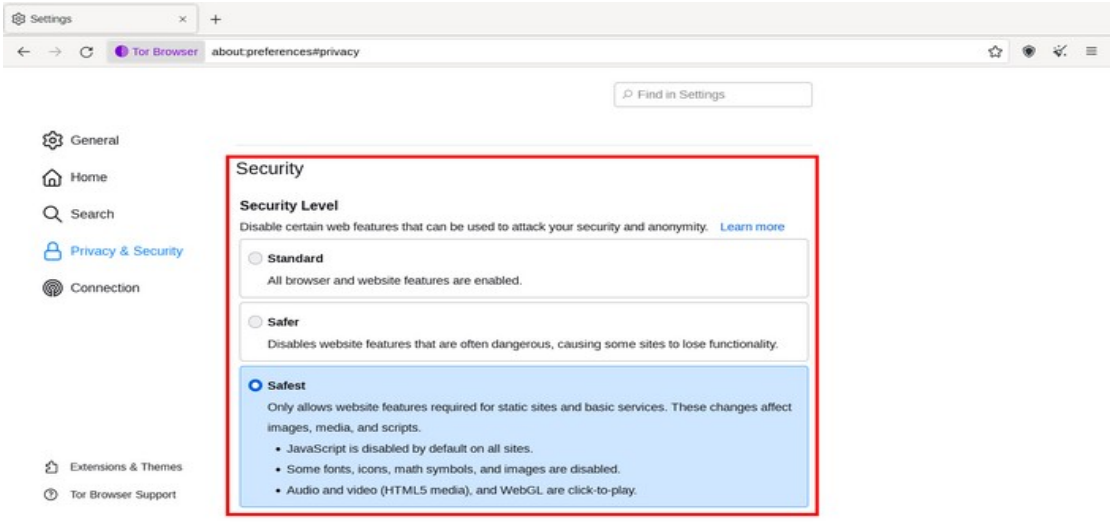
La funzione "Nuova identità" del browser Tor non è sufficiente a separare completamente le identità contestuali in Tails, in quanto non ristabilisce le connessioni al di fuori del browser Tor e si mantiene lo stesso nodo di ingresso Tor. Riavviare Tails è la soluzione migliore.



L'applicazione Onion Circuits mostra il circuito Tor utilizzato da una connessione server (sito web o altro). A volte può essere utile assicurarsi che il relay di uscita non si trovi in un determinato Paese, così da essere più lontani dall'accesso più facile per le autorità investigative. Nell'esempio sopra, la connessione a check.torproject.org passa attraverso i relay tor7kryptonit, Casper03 e il nodo di uscita blackfish. Cliccando su un circuito, nel riquadro di destra verranno visualizzati i dettagli tecnici sui suoi relay.

La funzione "Nuova identità" del browser Tor è utile per modificare il relay di uscita senza dover riavviare la sessione Tails; questa operazione può essere ripetuta fino a quando non si ottiene un relay di uscita soddisfacente. Si consiglia di utilizzare la funzione "Nuova identità" solo per modificare il nodo di uscita all'interno delle attività della stessa identità e non per passare da un'identità all'altra.

Impostazioni di sicurezza del browser Tor



Come qualsiasi software, anche il browser Tor presenta vulnerabilità† che possono essere sfruttate: diverse forze dell'ordine dispongono di exploit† per il browser Tor in casi gravi. Per mitigare questo rischio, è importante mantenere Tails aggiornato e aumentare le impostazioni di sicurezza del browser Tor: fai clic sull'icona dello scudo, quindi su "I**mpostazioni**". Per impostazione predefinita, l'impostazione è Standard, che garantisce un'esperienza di navigazione simile a quella di un browser tradizionale. **Si consiglia vivamente di impostarlo sul livello di sicurezza più restrittivo prima di iniziare la navigazione: "Il più sicuro"** (*Safest*). La stragrande maggioranza degli exploit contro il browser Tor non funzionerà con l'impostazione "Il più sicuro".

Il layout di alcune pagine potrebbe essere modificato e alcuni tipi di contenuto potrebbero essere disabilitati (immagini SVG, video click-to-play, ecc.). Ad esempio, anarsec.guide presenta due elementi che non funzionano in modalità "Il più sicuro" perché basati su JavaScript: la modalità scura e l'indice dell'articolo. Alcuni siti potrebbero non funzionare affatto con queste restrizioni; se hai motivo di fidarti di essi, puoi visualizzarli con un'impostazione meno restrittiva, valutando caso per caso. Ricorda che sia l'impostazione "Standard" che quella "Sicuro" consentono il funzionamento degli script che, nel peggiore dei casi, potrebbero compromettere il tuo anonimato[9].

Download/upload e cartella Tor Browser

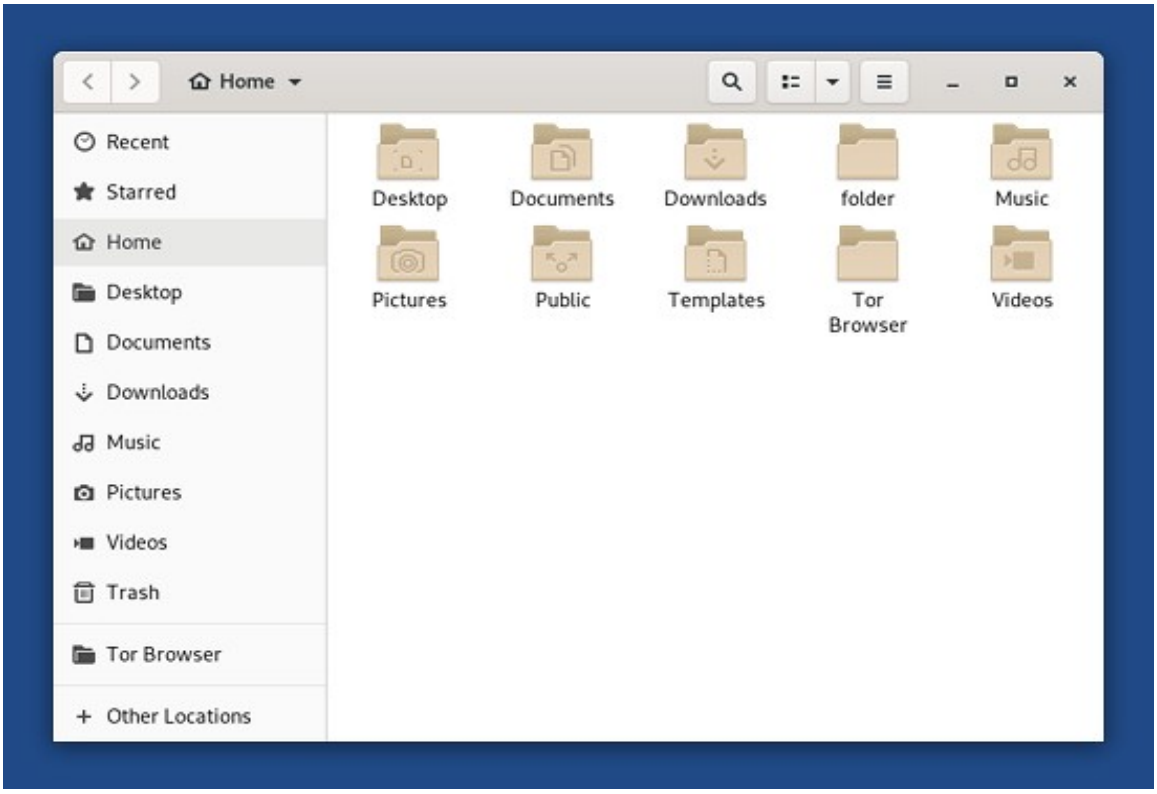
Il Tor Browser su Tails è conservato in una "sandbox†" per impedire che possa spiare tutti i tuoi file nel caso in cui un sito dannoso lo comprometta. Ciò significa che è necessario prestare particolare attenzione quando si caricano o scaricano file utilizzando il Tor Browser.

Download

Quando si scarica qualcosa utilizzando il Tor Browser, il file viene salvato nella cartella del Tor Browser (`/home/amnesia/Tor Browser/`) all'interno della sandbox. Se si desidera eseguire qualsiasi

9 https://arstechnica.com/information-technology/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/

operazione sul file, è necessario spostarlo dalla cartella del browser Tor. A tale scopo, puoi utilizzare il file manager (**Applicazioni > Accessori > File**).



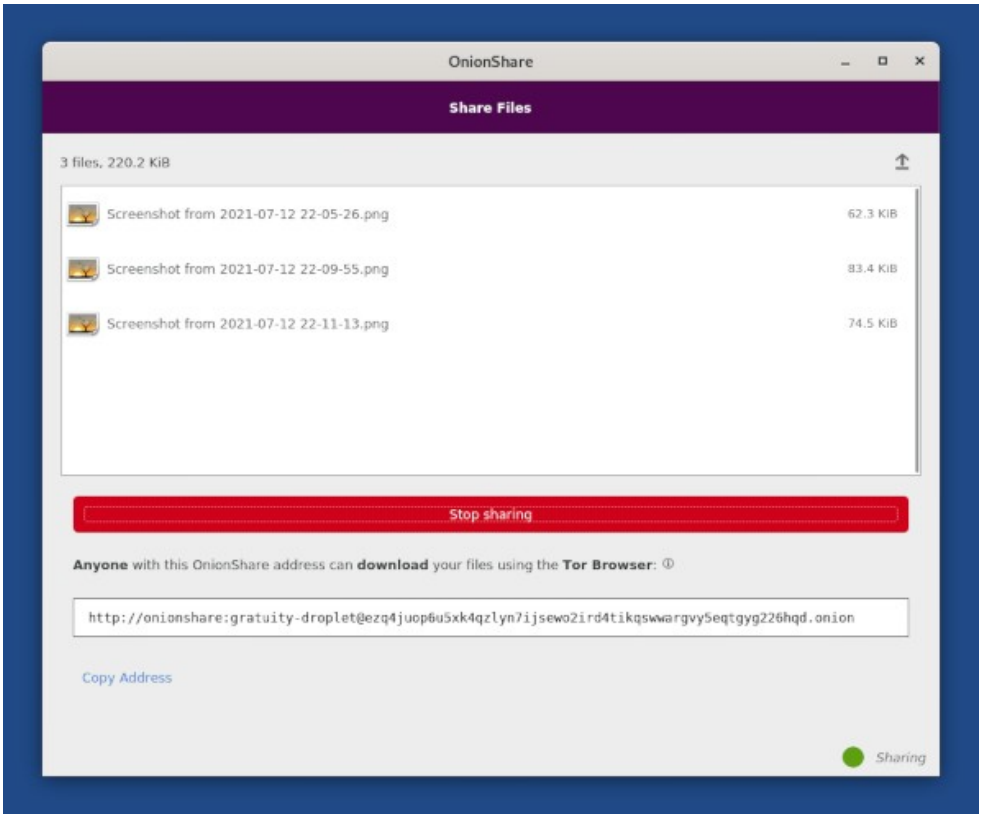
Upload

Allo stesso modo, se si desidera caricare qualcosa utilizzando il browser Tor (ad esempio, per includere un file in un post di un blog), è necessario prima spostare o copiare il file nella cartella del browser Tor. In questo modo, il file sarà disponibile quando si dovrà selezionare il file da caricare nel browser Tor.

RAM

È importante tenere presente che se si scaricano o si utilizzano file di grandi dimensioni, la RAM potrebbe riempirsi. Questo perché l'intera sessione di Tails viene eseguita nella RAM (a meno che non sia stata configurata la memoria persistente che utilizza la USB). Se la RAM si riempie, Tails potrebbe rallentare o bloccarsi. Per evitare questo problema, è possibile chiudere le applicazioni non necessarie ed eliminare gli altri file scaricati. Nel peggiore dei casi, potrebbe essere necessario abilitare temporaneamente la memoria persistente per scaricare o caricare file di grandi dimensioni tramite la cartella persistente del browser Tor che utilizza la USB anziché la RAM.

Condividi file con Onionshare



Grazie a OnionShare (**Applicazioni > Internet > OnionShare**) è possibile inviare un documento tramite un link .onion. Per impostazione predefinita, OnionShare interrompe il servizio nascosto dopo il primo download. Se si desidera offrire i file per più download, è necessario andare nelle impostazioni e deselezionare l'opzione "Interrompi la condivisione dopo il primo download". Non appena chiudi OnionShare, ti disconnetti da Internet o chiudi Tails, i file non saranno più accessibili. Questo metodo è ottimo per condividere file, perché non richiede di collegare una chiavetta USB al computer di qualcun altro, cosa che sconsigliamo di fare. L'indirizzo .onion, che è piuttosto lungo, può essere condiviso attraverso un altro canale (come un Riseup Pad[10] creato da te, che è più facile da digitare).

Rendere più difficili gli attacchi di correlazione†

Quando si richiede una pagina web tramite un browser web, il server del sito la invia in piccoli "pacchetti" che hanno una dimensione e una tempistica specifiche (tra le altre caratteristiche). Quando si utilizza il browser Tor, è anche possibile analizzare la sequenza dei pacchetti per cercare modelli che possano essere associati a quelli dei siti web. Per ulteriori informazioni, consulta “1.3.3. Modelli di traffico passivo a livello di applicazione”[11]. Tor prevede di risolvere questo problema in futuro[12].

Per rendere più difficile questo "attacco di correlazione†", disattiva JavaScript utilizzando Tor Browser con l'impostazione “**Il più sicuro**”.

10 pad.riseup.net/
11 https://spec.torproject.org/proposals/344-protocol-info-leaks.html
12 https://gitlab.torproject.org/tpo/team/-/wikis/Project-112?redirected_from=Sponsor-112

Inoltre, il team di Tor consiglia di eseguire più operazioni contemporaneamente con il client Tor[13].

Software inclusi

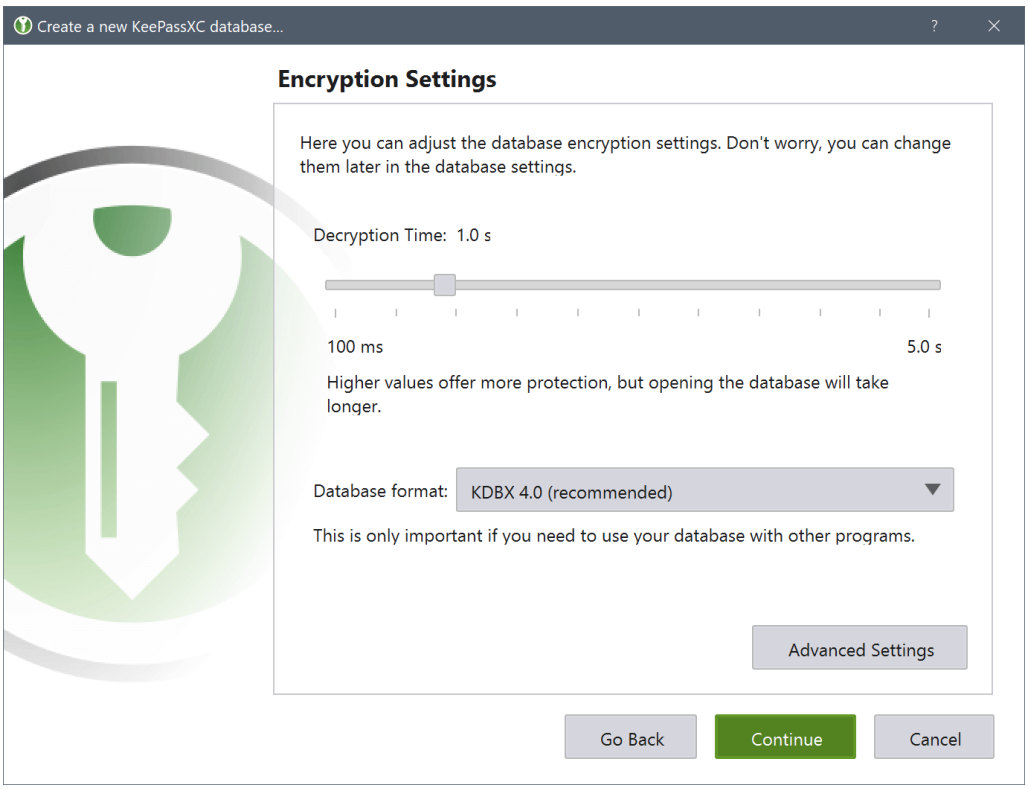
Tails include molte applicazioni di default. La documentazione fornisce una panoramica delle applicazioni Internet, delle applicazioni per la crittografia† e la privacy e delle applicazioni per la gestione di documenti sensibili. In questa sezione, metteremo in evidenza solo le applicazioni d'uso comune per l* anarchic*, ma per ulteriori informazioni si rimanda alla documentazione.

Gestore delle password (KeePassXC)

Quando è necessario ricordare molte password, può essere utile disporre di un metodo sicuro per memorizzarle (che non sia un foglio di carta accanto al computer). KeePassXC è un gestore di password incluso in Tails (**Applicazioni** > **Preferiti** > **KeePassXC**) che consente di memorizzare le password in un file e di proteggerle con un'unica password principale.

Si consiglia di suddividere le password in compartimenti: è necessario creare un file KeePassXC diverso per ogni singolo progetto/attività. È possibile utilizzare la stessa password principale [o *master*], ma lo scopo della suddivisione in compartimenti è quello di sbloccare le password di un progetto alla volta. Se la sessione di Tails viene compromessa, l'attaccante non otterrà tutte le password in un colpo solo, ma solo quelle attualmente sbloccate.

Nella terminologia di KeePassXC, una *password* è una sequenza casuale di caratteri (lettere, numeri e altri simboli), mentre una *passphrase* è una sequenza casuale di parole.



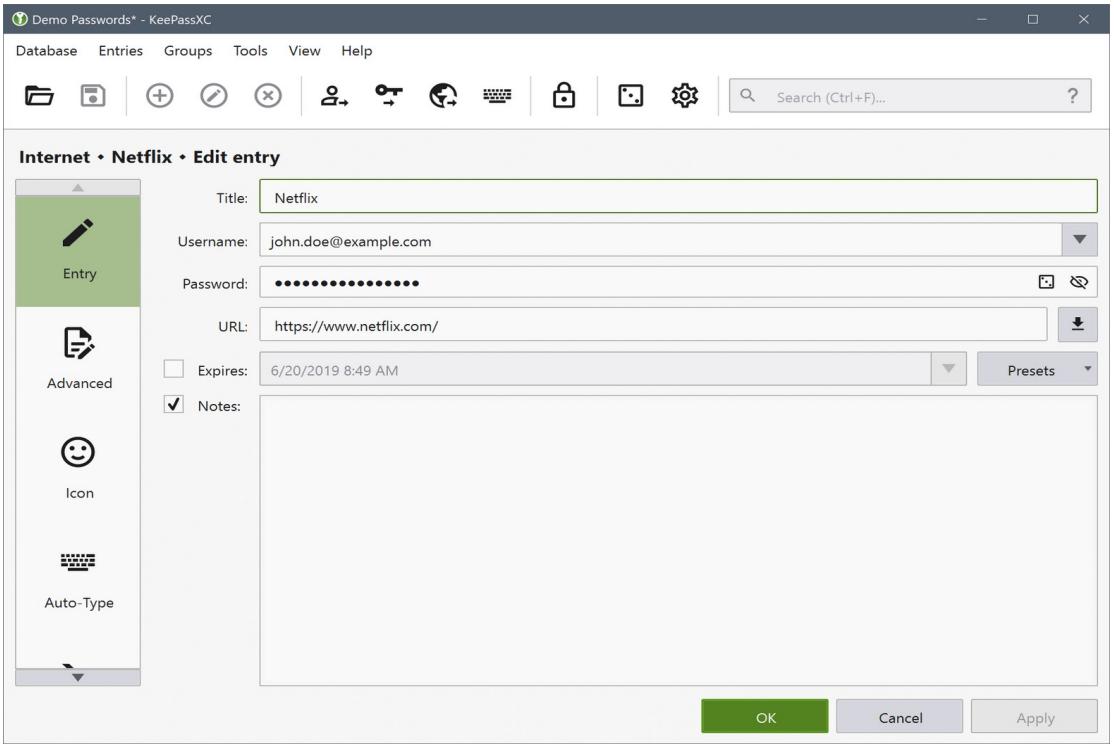
13 Poiché Tor utilizza connessioni criptate TLS per operare su circuiti multipli, un intruso che dovesse osservare dall'esterno il traffico di un cliente Tor dal nodo di "guardia" (entrata) avrà maggiori difficoltà a operarne una classificazione se quel cliente Tor sta facendo più cose contemporaneamente. Per maggiori informazioni: blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations/

Quando crei un nuovo database KeePassXC, aumenta il tempo di decrittazione nella finestra delle **Impostazioni di crittografia** dal valore predefinito al massimo (5 secondi). Quindi, scegli una passphrase complessa e salva il file KeePassXC. Ti consigliamo di fare clic sull'icona a forma di dado nel campo della password per generare una passphrase casuale composta da 7-10 parole.

Questo file del database KeePassXC conterrà tutte le tue password/passphrase e dovrà essere conservato tra una sessione e l'altra sul tuo Persistent Storage o su una chiavetta USB separata crittografata con LUKS†, come indicato nelle Best Practice di Tails. Non appena chiudi KeePassXC o non lo utilizzi per alcuni minuti, si bloccherà. Assicurati di non dimenticare la tua passphrase KeePassXC.

Dopo aver creato il database, dovresti vedere una cartella "Root" vuota. Se desideri organizzare le tue password in gruppi diversi, fai clic con il tasto destro del mouse su questa cartella e seleziona "Nuovo gruppo...".

Ora puoi aggiungere la tua prima voce. Fai clic su "**Voci**" e poi su "**Nuova voce**" oppure fai clic sull'icona "più". Inserisci il titolo dell'account, il nome utente e la password. Fai clic sull'icona “dado” per generare una password o una passphrase casuale per la voce.



Per copiare una password dal database, seleziona la voce e premi CTRL+C. Per copiare un nome utente, seleziona la voce e premi CTRL+B.

Eliminare definitivamente i dati da una chiavetta USB

Cliccando su "Elimina definitivamente" o inviando i file nel "Cestino" non si eliminano i dati... ed è molto facile recuperarli. Quando si elimina un file, si sta semplicemente comunicando al sistema operativo che non si è più interessati al suo contenuto. Il sistema operativo elimina quindi la voce del file

dall'indice dei file esistenti. Il sistema operativo può quindi riutilizzare lo spazio occupato dai dati per scrivere qualcos'altro.

Tuttavia, può essere necessario attendere settimane o anni prima che quello spazio venga effettivamente utilizzato per nuovi file e, a quel punto, i vecchi dati scompariranno. Nel frattempo, se si guarda direttamente ciò che è scritto sull'unità, è possibile trovare il contenuto dei file. Si tratta di un processo piuttosto semplice, automatizzato da molti programmi software che consentono di "recuperare" o "ripristinare" i dati. Non è possibile cancellare i dati in modo definitivo, ma è possibile sovrascriverli, il che rappresenta una soluzione parziale.

Esistono due tipi di archiviazione: magnetica (HDD) e flash (SSD, NVMe, USB, schede di memoria, ecc.). L'unico modo per cancellare un file su entrambi è riformattare l'intero disco e selezionare "**Sovrascrivi i dati esistenti con zeri**".

Tuttavia, potrebbero rimanere tracce dei dati precedentemente scritti. Se si desidera cancellare in modo definitivo documenti sensibili, è meglio distruggere fisicamente l'USB dopo averlo riformattato. Fortunatamente, le chiavette USB sono economiche e facili da rubare. È importante riformattare l'unità prima di distruggerla, perché la distruzione di un'unità è spesso una soluzione parziale. I dati possono ancora essere recuperati dai frammenti del disco e, per distruggere un'unità, sono necessarie temperature superiori a quelle di un normale incendio (ad esempio, la termite).

Per le unità di memoria flash (come le chiavette USB, gli SSD, le schede SD, ecc.) è necessario rompere il circuito stampato dall'involucro di plastica utilizzando delle pinze. Per sminuzzare i chip di memoria, compreso il circuito stampato, in pezzi di dimensioni inferiori a due millimetri, utilizzare un frullatore domestico di alta qualità. Questo frullatore non deve essere utilizzato in seguito per gli alimenti, perché la pulizia non rimuove adeguatamente le tracce tossiche.

Come creare una USB crittografata

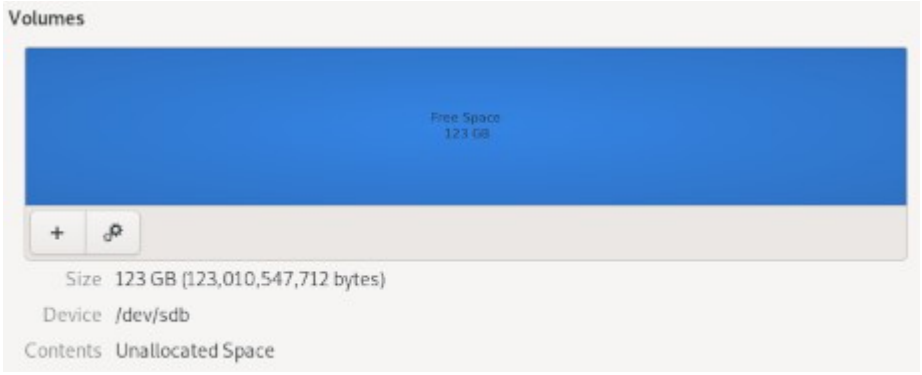
Archivia i dati solo su unità crittografate. Ciò è necessario se desideri utilizzare una USB LUKS† separata invece della memoria permanente sulla USB Tails, come consigliato nelle migliori pratiche di Tails. LUKS† è lo standard di crittografia Linux. Per crittografare una nuova USB, vai su **Applicazioni → Utilità → Dischi**.

- Quando inserisci la USB, dovrebbe apparire un nuovo “dispositivo” nell'elenco. Selezionalo e assicurati che la descrizione (marca, nome, dimensione) corrisponda al tuo dispositivo. Fai attenzione a non commettere errori!
- Formattalo cliccando su ≣ → **Formatta il disco**.

- Nell'elenco a discesa Cancella, seleziona **Sovrascrivi i dati esistenti con zeri**. Tieni presente che questo non è sufficiente per rimuovere tutte le tracce dei documenti sensibili memorizzati sull'USB.

- Nell'elenco a discesa Partizionamento, seleziona **Compatibile con tutti i sistemi e dispositivi (MBR/DOS)** .

- Quindi clicca su **Formatta**…



- Ora è necessario aggiungere la partizione crittografata.

- Fare clic sul pulsante “+”

- Selezionare la dimensione della partizione (tutto lo spazio libero)

- Per “Tipo” selezionare **disco interno da utilizzare solo con sistemi Linux (Ext4)**; selezionare **Volume protetto da password (LUKS†)**

- Immettere una passphrase complessa

Se inserisci una USB crittografata, ti verrà richiesto di inserire la passphrase. Prima di rimuovere l'unità dopo aver terminato di lavorarci, devi fare clic con il pulsante destro del mouse su **Home→ Computer** e selezionare **Espelli**.

Crittografare un file con una password o una chiave pubblica

In Tails, puoi utilizzare l'applicazione Kleopatra per crittografare un file con una password o una chiave PGP pubblica. Questo crea un file .pgp. Se si desidera crittografare un file, farlo nella RAM prima di salvarlo su una USB LUKS†. Una volta che la versione non crittografata di un file è stata salvata su una USB, la USB deve essere riformattata per rimuoverla.

Per lo stesso motivo, prima di decrittografare un file, copiarlo prima in una cartella Tails che si trova solo nella RAM (ad esempio **Home → Documenti)**.

Aggiungere i diritti di amministrazione

Tails richiede una password di amministrazione (chiamata anche "password root") per eseguire attività di amministrazione del sistema. Ad esempio:

- installazione di software aggiuntivo;
- accesso ai dischi rigidi interni del computer;
- esecuzione di comandi nel terminale root;
- accesso a determinati privilegi, ad esempio quando viene visualizzata una finestra che richiede l'autenticazione di amministrazione.

Per impostazione predefinita, la password di amministrazione è disabilitata per motivi di sicurezza. Ciò può impedire a un malintenzionato, che abbia accesso fisico† o remoto† al sistema Tails, di ottenere i privilegi di amministrazione. Se si imposta una password di amministrazione per la sessione, si crea un altro vettore che potenzialmente consente di aggirare la sicurezza di Tails.

Per impostare una password di amministrazione, è necessario selezionarla nella schermata di benvenuto all'avvio di Tails. Questa password è valida solo per la durata della sessione.

Installazione di software aggiuntivo

Se installi un nuovo software, spetta a te assicurarti che sia sicuro. Tails obbliga tutti i software a connettersi a Internet tramite Tor, pertanto dovrai configurare le applicazioni che utilizzano Internet. Il software utilizzato in Tails è sottoposto a controlli di sicurezza, ma questo potrebbe non essere il caso di quello che installerai. Prima di installare un nuovo software, è meglio assicurarsi che Tails non disponga già di un software in grado di svolgere la funzione desiderata. Se desideri che il software aggiuntivo rimanga attivo anche dopo la chiusura della sessione, devi abilitare l'opzione "Software aggiuntivo" nella configurazione dell'archiviazione persistente.

Per ulteriori informazioni, consulta la documentazione sulla pagina di Tails sull'installazione di software aggiuntivo.

Ricordati di fare dei backup!

Una chiavetta USB Tails può essere facilmente smarrita e le chiavette USB hanno una durata molto inferiore rispetto agli hard disk, soprattutto quelle economiche. Se contengono dati importanti, ricordati di eseguire regolarmente il backup. Se utilizzi una seconda chiavetta USB crittografata con LUKS†, puoi copiare i file su una chiavetta USB di backup crittografata con LUKS direttamente dal File Manager.

Se utilizzi Persistent Storage, consulta la documentazione sulla pagina di Tails per eseguire il backup.

Schermo per la privacy

È possibile aggiungere uno schermo per la privacy[14] al monitor del laptop per impedire alle persone (o alle telecamere nascoste) di vedere il contenuto, a meno che non si trovino direttamente di fronte a esso.

III) Risoluzione dei problemi

Il computer tenta di avviare l'USB, ma senza successo.

Controlla i messaggi di errore che ricevi (ad esempio, se il tuo computer è a 32 bit, non sarà compatibile con Tails). Se viene visualizzato il messaggio "`Errore durante l'avvio di GDM con la scheda grafica`", il problema riguarda la scheda grafica; consulta la documentazione relativa ai problemi noti con le schede grafiche. Puoi anche consultare l'elenco dei problemi noti sul sito di Tails relativo al tuo modello di computer.

Se appare la pagina Tails Boot Loader, prova ad avviare Tails in modalità di risoluzione dei problemi.

La mia chiavetta USB Tails non si avvia più! (e prima si avviava sullo stesso computer).

14 Si tratta di un filtro o pannello fisico da applicare al monitor del computer/tablet/smartphone (si fissa generalmente tramite strisce adesive o si fa scorrere in posizione) che funziona grazie a micro-riflettori, ovvero piccole tende veticali integrate nel filtro dello schermo, angolate in modo tale da consentire di vedere chiaramente il display solo all'utente seduto direttamente di fronte allo schermo, oscurando la vista dagli angoli laterali. Si trovano in vendita a modico prezzo, NdT.

Dopo un aggiornamento o altro, Tails non si avvia più sul tuo computer. Hai tre opzioni:

1. Controlla se la pagina delle news di Tails menziona eventuali problemi con l'aggiornamento;
2. Esegui un aggiornamento manuale, che potrebbe essere necessario se il computer è stato spento prima del completamento dell'aggiornamento automatico.
3. Se nessuna delle due soluzioni funziona, l'USB potrebbe essere troppo vecchia, di scarsa qualità o danneggiata. Se hai bisogno di recuperare i dati dalla memoria persistente, collega l'USB a una sessione Tails utilizzando un'altra USB. Apparirà come una normale USB che dovrai sbloccare con la tua password. Se non riesci ad accedere ai tuoi dati su un'altra USB Tails con la persistenza abilitata, la tua USB potrebbe essere rotta.

Non riesco a collegarmi a una rete Wi-Fi pubblica con una pagina di autenticazione (un captive portal).

Se devi connetterti a una rete Wi-Fi pubblica che richiede l'autenticazione tramite un portale, devi abilitare il "Browser non sicuro" dalla schermata di benvenuto. Connettiti alla rete Wi-Fi, quindi apri **Applicazioni > Internet > Browser non sicuro**. Inserisci l'URL di un sito affidabile (ad esempio, Wikipedia) per accedere alla pagina di autenticazione. Una volta completata la pagina del captive portal, attendi che Tor sia pronto, quindi chiudi il browser non sicuro.

Cosa succede se esaurisco lo spazio su una chiavetta USB?

Se esaurisci lo spazio su un'unità USB o se visualizzi meno dati rispetto a quelli effettivamente presenti sull'unità, seleziona "Mostra file nascosti" nel browser dei file. Lì vedrai nuovi file denominati `.qualcosa`. Il file `.Trash-10xx` occupa spazio: se fai clic con il tasto destro del mouse su di esso e selezioni "Sposta nel cestino", verrà rimosso completamente. Non modificare nessun altro file nascosto.

Un file si apre sempre in modalità di sola lettura o non si apre affatto?

In alcuni programmi, questo è normale se lo stesso file è già aperto. Se non è questo il caso, usa lo stesso trucco descritto nel paragrafo precedente. Abilita "Mostra file nascosti". Ci sarà un file .lock con lo stesso nome del file che ti crea problemi. Elimina questo file, che indica che il file è già aperto altrove. Se il problema persiste, devi modificare i diritti di accesso al file.

Non riesco a installare Tails su una chiavetta USB.

Verifica che la tua USB non presenti problemi noti con Tails. Formatta l'intera USB e riprova l'installazione.

Un'applicazione sta rallentando Tails? Lo schermo presenta dei disturbi?

Prova a premere il tasto Windows o il tasto Cmd su Mac, che aprirà una finestra con tutte le applicazioni in esecuzione e ti permetterà di chiuderle. Se questo metodo non funziona, dovrai forzare lo spegnimento tenendo premuto il pulsante di accensione.

Aggiungi una stampante.

Vai su "**Applicazioni" > "Strumenti di sistema" > "Impostazioni" > "Dispositivi" > "Stampanti" > "+" > "Aggiungi una stampante**". Alcuni modelli di stampante potrebbero non essere compatibili con Tails (o potrebbero essere difficili da configurare).

Impossibile installare nuovo software.

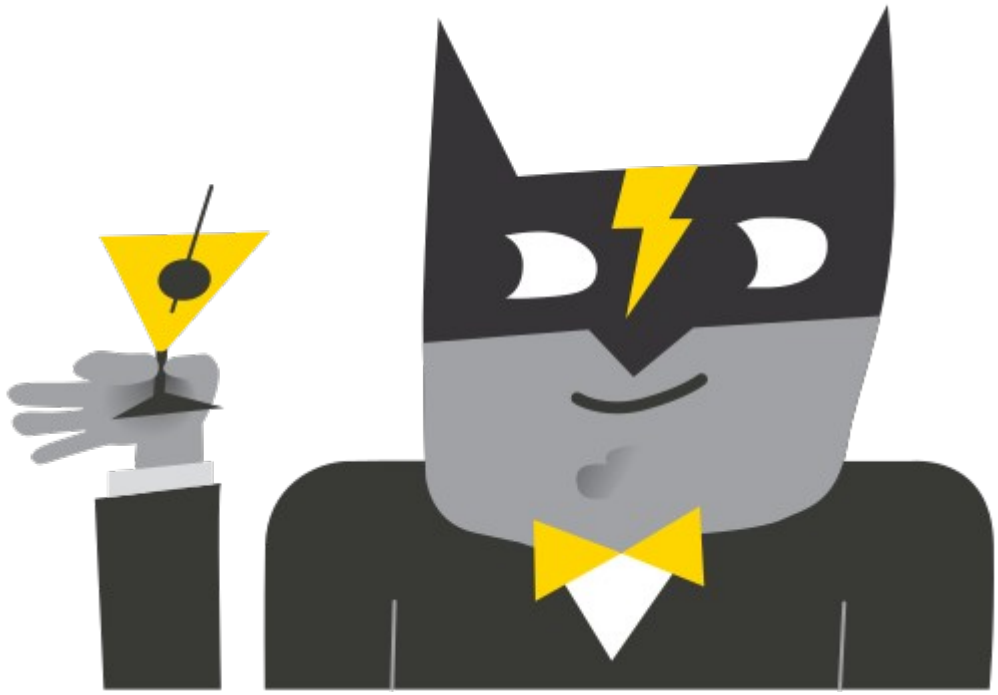
A volte, Synaptic Package Manager rifiuta di installare il software. In questo caso, usa un terminale root (che richiede una password di amministrazione): installa con il comando `apt update && apt install [nome_pacchetto]`

Migliori pratiche di Tails

Tutt* l* anarchic* dovrebbero sapere come usare Tails. Questo testo descrive alcune precauzioni aggiuntive che è possibile adottare e che sono rilevanti per il rischio repressivo in cui incorrono l* anarchic*. Non tutti i “modelli di rischio” sono uguali e solo tu puoi decidere quali misure di mitigazione adottare per le tue attività, ma il nostro obiettivo è fornirti consigli adeguati per attività ad alto rischio, come la rivendicazione di un'azione..

Inizieremo esaminando i tre argomenti trattati nella pagina "Avvertenze" di Tails: la protezione della tua identità, i limiti della rete Tor e i computer non affidabili.

Proteggere la propria identità quando si utilizza Tails



Tails è progettato per nascondere l'identità dell'utente. Tuttavia, alcune attività potrebbero rivelarla:

1. condivisione di file con metadati quali data, ora, posizione e informazioni sul dispositivo;
2. utilizzo di Tails per più di uno scopo alla volta.

1. Condivisione di file con metadati

Per mitigare questo problema, è possibile **pulire i metadati dai file prima di condividerli.**

Per sapere come fare, consulta la guida Rimuovere i metadati identificativi dai file (in appendice).

2. Utilizzo di Tails per più di uno scopo alla volta

È possibile mitigare questo secondo problema con la cosiddetta "**compartimentazione**".

- La compartimentazione consiste nel mantenere separate attività o progetti diversi. Se si utilizzano sessioni Tails per più scopi contemporaneamente, un malintenzionato potrebbe mettere in relazione le diverse attività. Ad esempio, se si accede a account diversi sullo stesso sito web in una singola sessione Tails, il sito web potrebbe dedurre che gli account sono utilizzati dalla stessa persona. Ciò è possibile perché i siti web sono in grado di rilevare quando due account utilizzano lo stesso circuito Tor.
- Per impedire a un malintenzionato di collegare le tue attività mentre utilizzi Tails, riavvia Tails tra un'attività e l'altra. Ad esempio, riavvia Tails tra un controllo e l'altro delle e-mail di progetti diversi.
- Tails è amnesico per impostazione predefinita, quindi, per salvare i dati di una sessione Tails, è necessario salvarli su una chiavetta USB. Se i file salvati potrebbero essere utilizzati per collegare le tue attività, utilizza una chiavetta USB crittografata (LUKS†) diversa per ogni attività. Per esempio, usa una chiavetta USB Tails per moderare un sito web e un'altra per la ricerca di azioni. Tails dispone di una funzione chiamata "Archiviazione Persistente", ma non consigliamo di utilizzarla per l'archiviazione dei dati, come spiegheremo di seguito.

Limiti della rete Tor

Tails utilizza la rete Tor perché è la più potente e popolare per proteggersi dalla sorveglianza e dalla censura. Tuttavia, Tor presenta alcuni limiti:

1. Nascondere che si sta utilizzando Tor e Tails;

2. Proteggere le tue comunicazioni online da aggressori determinati ed esperti.

1. Nascondere l'utilizzo di Tor e Tails

Per mitigare questo problema, puoi utilizzare i bridge Tor.

- I bridge Tor sono relay Tor segreti che nascondono la tua connessione alla rete Tor. Tuttavia, ciò è necessario solo quando le connessioni a Tor sono bloccate, ad esempio in paesi con una forte censura, su alcune reti pubbliche o su alcuni software di controllo parentale. Questo perché Tor e Tails non ti fanno sembrare un utente Internet qualsiasi, ma fanno sembrare tutti gli utenti Tor e Tails uguali. Diventa impossibile distinguere chi è chi.[15]

2. Protezione contro attacchi determinati e sofisticati

Un attacco di correlazione *end-to-end†* è un metodo teorico con cui un potente avversario potrebbe violare l'anonimato di Tor.

> “Un potente avversario, in grado di analizzare i tempi e la forma del traffico in entrata e in uscita dalla rete Tor, potrebbe essere in grado di rendere identificabili gli utenti di Tor. Questi attacchi sono chiamati "*attacchi di correlazione end-to-end*" perché l'attaccante deve osservare entrambe le estremità di un circuito Tor nello stesso momento […]. Gli attacchi correlati end-to-end sono stati studiati in lavori di ricerca, ma non siamo a conoscenza di un uso effettivo per togliere l’anonimato agli utenti Tor.”[16]

Attacchi di correlazione non mirati e mirati

Come descritto nella citazione precedente, un avversario potente (come la NSA) potrebbe essere in grado di violare Tor attraverso un attacco di correlazione. Se ciò accadesse, l'indirizzo Internet che hai utilizzato in un bar senza telecamere a circuito chiuso porterebbe solo alla tua zona generale (ad esempio, alla tua città), perché non è associato a te. Naturalmente, questo è meno vero se si utilizza quella posizione abitualmente. Gli attacchi di correlazione sono ancora meno fattibili contro le connessioni a un indirizzo .onion, perché non si esce mai dalla rete Tor e non c'è una "fine" da correlare attraverso l'analisi del traffico di rete (se la posizione del server è sconosciuta all’attaccante).

Un attacco di correlazione "mirato" è molto più probabile, perché un avversario non globale (ad esempio le forze dell'ordine locali) può compierlo se sei già nel suo mirino e sei oggetto di sorveglianza fisica e/o digitale. Si tratta di un sottotipo di attacco di correlazione in cui il presunto bersaglio è già noto, il che rende l'attacco più facile da realizzare, in quanto riduce notevolmente la quantità di dati da filtrare per la correlazione. Un attacco di correlazione non mirato, utilizzato per rendere identificabile un utente Tor, non ha precedenti nelle prove attualmente utilizzate in tribunale, anche se un attacco di correlazione "mirato" è stato utilizzato come prova incriminante[17]: una persona sotto indagine era già stata identificata e questo ha permesso agli investigatori di correlare le tracce osservate con specifiche attività online. In particolare, hanno correlato il traffico di rete Tor proveniente dall'abitazione dell’indagat* con gli orari in cui il suo alias anonimo era online nelle chat room.

15 Ciò significa che se non ci si connette da paesi che censurano Tor (Cina, Russia, Bielorussia ad es.) non è strettamente necessario richiedere un bridge che funzioni per quei paesi, a meno che non si voglia in ogni caso nascondere il fatto che si sta utilizzando Tor, NdT.

16 https://www1.tails.net/doc/about/warnings/tor/index.it.html#correlation

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

Per capire come funziona, è utile avere una conoscenza di base delle informazioni visibili a varie terze parti su Tor. Per un attacco di correlazione non mirato, l'investigatore deve *partire da dopo il nodo di uscita di Tor* e cercare di correlare la specifica attività online proveniente da tale nodo con un'enorme quantità di dati globali che entrano nei nodi di ingresso di Tor. Tuttavia, se l'indagat* è già stat* identificat*, l'investigatore può effettuare un attacco di correlazione "mirato" e partire da *prima del nodo di ingresso di Tor*: i dati che entrano nel nodo di ingresso (tramite l'*impronta fisica o digitale* dell'indagat*) vengono messi in correlazione con una *specifica attività online* proveniente da un nodo di uscita.

Per quanto riguarda la tua *impronta fisica*, un'operazione di sorveglianza potrebbe notare che frequenti regolarmente un bar e cercare di correlare questo dato con l'attività online di cui sei sospettato (ad esempio, se sospettano che tu stia gestendo un sito, potrebbero cercare di correlare queste finestre temporali con l'attività di moderazione del sito). Per quanto riguarda la tua *impronta digitale*, se ti connetti a Internet da casa, un investigatore può monitorare tutto il tuo traffico Tor e cercare di metterlo in relazione con l'attività online di cui sei sospettat*. Per quanto riguarda la tua *attività online specifica*, un'analisi più sofisticata comporterebbe la registrazione delle connessioni al server per un confronto dettagliato, mentre un'analisi più semplice renderebbe visibili a chiunque i dati pubblicamente disponibili (come quando il tuo alias è online in una chat room o quando un post viene pubblicato su un sito web).

Per mitigare le tecniche a disposizione di avversari potenti, puoi **dare la priorità ai link .onion quando disponibili, tenere conto della possibilità di una sorveglianza mirata e utilizzare una connessione Internet non associata alla tua identità**.

Una connessione Internet non collegata alla tua identità

Utilizzare una connessione Internet non collegata alla propria identità significa che, anche in caso di attacco alla rete Tor, la propria identità rimarrebbe comunque anonima. Ci sono due opzioni: utilizzare il Wi-Fi di uno spazio pubblico (come un bar senza telecamere a circuito chiuso) o utilizzare un'antenna Wi-Fi attraverso una finestra da uno spazio privato.

Lavorare in un luogo pubblico

Se hai bisogno di utilizzare Internet solo occasionalmente, per esempio per inviare un comunicato o fare delle ricerche sul campo, **puoi fare un controllo per individuare sistemi sorveglianza e prendere contromisure prima di andare in un internet café,** proprio come faresti prima di un'azione diretta. Per ulteriori informazioni su cosa comporta l'invio di un comunicato, consulta "Come inviare un comunicato anonimo e farla franca".[18]

Quando si utilizza il Wi-Fi in un luogo pubblico, è necessario tenere a mente le seguenti considerazioni relative alla sicurezza operativa:

- Il tempismo è un fattore importante da considerare. Se volete inviare un resoconto la mattina dopo una rivolta o un comunicato poco dopo un'azione (momenti in cui c'è un rischio maggiore di sorveglianza mirata), valutate l'idea di aspettare. Nel 2010, la mattina dopo un attacco incendiario in una banca in Canada, la polizia ha sorvegliato un sospettato mentre si recava dalla sua abitazione a un internet café, lo ha osservato mentre pubblicava la rivendicazione e poi seppelliva il laptop nel bosco. Più recentemente, gli investigatori che sorvegliavano fisicamente un anarchico

18 https://www.notrace.how/resources/read/how-to-submit-an-anonymous-communique.html

in Francia[19] hanno installato una telecamera nascosta per monitorare l'accesso a un internet café vicino alla casa del compagno e hanno richiesto le riprese delle telecamere a circuito chiuso del giorno in cui è stata inviata la rivendicazione di un attacco incendiario.

- Se possibile, evitate di frequentare sempre gli stessi internet café. Più un luogo viene utilizzato regolarmente, più Internet è legato alla propria identità. Inoltre, se un'operazione di sorveglianza conosce la tua destinazione, le misure di controsorveglianza non saranno efficaci.
- Se devi acquistare un caffè per ottenere la password del Wi-Fi, paga in contanti!
- Posizionati con le spalle contro un muro, in modo che nessuno possa "spiare" il tuo schermo, e installa idealmente uno schermo per la privacy sul tuo laptop. Se scrivi un comunicato in una sessione offline di Tails prima di recarti in uno spazio pubblico, ti basteranno pochi minuti in un bagno pubblico per inviarlo.
- Se i bar senza telecamere a circuito chiuso sono pochi e distanti tra loro, puoi provare ad accedere al Wi-Fi di un bar dall'esterno, fuori dalla portata delle telecamere.
- Mantieni la consapevolezza della situazione e sii pront* a rimuovere la chiavetta USB Tails per spegnere il computer in qualsiasi momento. È difficile mantenere un'adeguata consapevolezza della situazione rimanendo concentrat* sulla sessione Tails: valuta la possibilità di chiedere a un amic* fidat* di rimanere con te e di tenere d'occhio ciò che accade intorno a te. Se la chiavetta USB viene rimossa, Tails si spegnerà e sovrascriverà la RAM con dati casuali. Tutte le chiavette USB LUKS sbloccate durante la sessione Tails verranno nuovamente crittografate. Si noti che Tails avverte: "Rimuovere fisicamente la chiavetta USB solo in caso di emergenza, poiché ciò può talvolta danneggiare il file system dell’archivio persistente".

A una persona responsabile di un mercato darknet è stato sequestrato il computer Tails mentre era distratt* da una rissa simulata nelle sue vicinanze. Tattiche simili sono state utilizzate in altre operazioni di polizia[20]. Se la sua chiavetta USB Tails fosse stata fissata alla cintura con un breve pezzo di lenza da pesca, la polizia avrebbe perso tutte le prove nel momento di espulsione della chiavetta. Un'alternativa più tecnica è BusKill, ma consigliamo di acquistarlo solo di persona o di stamparlo in 3D. Questo perché qualsiasi spedizione postale può essere intercettata e manomessa, rendendo l'hardware pericoloso.

Lavorare in un luogo privato

Se avete bisogno di utilizzare regolarmente Internet per progetti come la moderazione di un sito web o l'hacking, spostarsi in una nuova posizione Wi-Fi dopo aver adottato contromisure di sorveglianza potrebbe non essere realizzabile quotidianamente. Inoltre, una delle principali priorità della polizia sarà quella di sequestrare il computer mentre non è crittografato e questo è molto più facile da realizzare in uno spazio pubblico, soprattutto se siete da sol*. In questo scenario, la soluzione ideale è **utilizzare un'antenna Wi-Fi posizionata dietro una finestra in uno spazio privato per accedere da alcune centinaia di metri di distanza**: una sorveglianza fisica non ti osserverà mentre entri in un bar e non potrà sequestrare facilmente il tuo laptop acceso, mentre una sorveglianza digitale non potrà osservare nulla sulla tua rete Internet domestica. Per proteggersi dalle telecamere nascoste, è comunque necessario fare attenzione a dove si posiziona lo schermo.

19 https://www.notrace.how/resources/#ivan
20 https://dys2p.com/en/2023-05-luks-security.html#attacks

Se un'antenna Wi-Fi è troppo tecnica per te, potresti comunque voler usare **la tua connessione Internet domestica** per alcuni progetti che richiedono un accesso frequente a Internet. Ciò contraddice il consiglio precedente di non utilizzare una connessione Internet associata alla tua identità. Si tratta di un compromesso: utilizzare Tor da casa evita di creare un'impronta fisica così facile da osservare, a scapito però della creazione di un'impronta digitale che è più difficile da osservare e dalla quale potrebbe essere più difficile trarre conclusioni significative. Ci sono due rischi principali di perdita di anonimato da considerare quando si utilizza la connessione Internet di casa: che l'avversario scopra la tua identità tramite un attacco di correlazione† Tor o che lo faccia hackerando il tuo sistema (ad esempio tramite phishing†), il che gli permetterebbe di aggirare Tor. Per rendere entrambi questi attacchi più difficili, si consiglia di connettersi a una VPN† prima di connettersi a Tor (cioè Tu → VPN → Tor → Internet), quando si utilizza Tails da casa. Ciò richiede l'esecuzione della VPN dal proprio dispositivo di rete (un router o un firewall hardware). Per ulteriori informazioni sulla logica alla base di questa scelta, consulta le Guide sulla privacy di Tor[21].

Riassumendo:

Per attività Internet sensibili e irregolari, è meglio utilizzare una connessione Wi-Fi di un bar a caso, dopo aver effettuato un rilevamento della sorveglianza e adottato misure di controsorveglianza. Per le attività che richiedono un accesso quotidiano a Internet, per cui non è realistico adottare contromisure di sorveglianza e trovare un nuovo bar, è meglio utilizzare un'antenna Wi-Fi. Se questo è troppo tecnico per te, puoi usare il Wi-Fi di casa, ma ciò richiede che tu abbia fiducia nella capacità di Tor di resistere agli attacchi di correlazione, nelle misure che hai adottato per proteggerti dagli hacker e nel tuo provider VPN.

Ridurre i rischi quando si utilizzano computer non affidabili

21 https://www.privacyguides.org/en/advanced/tor-overview/#safely-connecting-to-tor

Tails può essere eseguito in modo sicuro su un computer infetto. Tuttavia, Tails non può sempre proteggerti quando:

1. Si esegue l'installazione da un computer infetto;
2. Si esegue Tails su un computer con BIOS, firmware o hardware compromessi.

1. Installazione da un computer infetto

Per mitigare questo problema, è possibile **installare Tails con un computer di cui ti fidi:**

- Secondo le nostre raccomandazioni, l'ideale sarebbe un sistema Qubes OS†, in quanto è molto più difficile da infettare rispetto a un normale computer Linux.
- Utilizza il metodo di installazione "Terminale" "Debian o Ubuntu utilizzando la riga di comando e GnuPG†", che verifica in modo più approfondito l'integrità del download utilizzando GPG. Se l'uso della riga di comando ti risulta troppo complicato, impara le basi con Linux Essentials.
- Una volta installato, non collegare la chiavetta USB Tails (o qualsiasi USB LUKS utilizzata durante le sessioni Tails) ad altri computer, perché se il computer è infetto, l'infezione potrebbe diffondersi alla chiavetta USB.

2. Esecuzione di Tails su un computer con BIOS, firmware o hardware compromessi.

Questo secondo problema richiede diverse misure di mitigazione. Iniziamo con alcune definizioni.

- Il *software* è costituito da istruzioni per il computer scritte in "codice".
- L'*hardware* è il computer fisico che state utilizzando.
- Il *firmware* è un software di basso livello incorporato in un componente hardware e può essere considerato come il collante tra l'hardware e il software di livello superiore del sistema operativo. Si trova in diversi componenti (dischi rigidi, unità USB, processore grafico, ecc.).
- Il *BIOS* è il firmware specifico incorporato nell'hardware della scheda madre e responsabile dell'avvio del computer quando si preme il pulsante di accensione.

I nostri avversari hanno due categorie di vettori di attacco: gli attacchi fisici, che avvengono tramite accesso fisico, e gli attacchi remoti, che avvengono tramite accesso remoto a Internet. Un avversario con accesso fisico può compromettere il software (ad esempio sostituendo il sistema operativo con una versione dannosa), l'hardware (ad esempio aggiungendo un keylogger) e il firmware (ad esempio sostituendo il BIOS con una versione dannosa). Un avversario con accesso remoto inizia hackerando il software (compromettendolo) e può quindi passare a compromettere il firmware.

Se un avversario ha compromesso l'hardware o il firmware di un laptop, ciò comprometterebbe anche una sessione Tails, in quanto il sistema operativo funzionerebbe su una base danneggiata.

Non tutti i consigli riportati di seguito sono necessari. Ad esempio, se si utilizza Tails solo per la navigazione web anonima e la corrispondenza scritta, alcuni di questi consigli potrebbero essere eccessivi. Tuttavia, se si utilizza Tails per rivendicare azioni altamente criminalizzate, è probabilmente opportuno adottare un approccio più accurato.

Per mitigare gli attacchi fisici:

- In primo luogo, è necessario **procurarsi un computer nuovo**. È improbabile che un laptop acquistato in un negozio di computer ricondizionati a caso sia già stato compromesso. Acquistare il computer in contanti, in modo da non poter risalire all'acquirente, e di persona, perché la posta può essere intercettata. Un Thinkpad usato è un'opzione economica e affidabile. È meglio utilizzare Tails su un laptop dedicato, in modo da impedire all'avversario di prendere di mira il firmware attraverso un sistema operativo meno sicuro o attraverso le normali attività non anonime. Un altro motivo per avere un laptop dedicato è che, se qualcosa in Tails si rompe, qualsiasi informazione che ne fuoriesce e lo espone non sarà automaticamente collegata a te e alle tue normali attività al computer.

Rendi le viti del laptop a prova di manomissione [*tamper-evident*], conservalo in un luogo sicuro e monitora eventuali effrazioni. Con queste precauzioni, sarai in grado di rilevare eventuali attacchi fisici futuri. Per adattare le viti del tuo laptop, utilizzare qualche forma di rilevamento delle intrusioni e conservare il tuo computer in modo adeguato, consulta la guida "Rendi i tuoi dispositivi elettronici a prova di manomissione[22]". Conserva allo stesso modo tutti i dispositivi esterni che utilizzerai con il laptop (chiavette USB, dischi rigidi esterni, mouse e tastiere). Quando i vettori di attacco fisico sono mitigati, un avversario può solo utilizzare attacchi remoti.

Per mitigare gli attacchi remoti:

- **Utilizza una rete Wi-Fi che non sia collegata alla tua identità**. Questo consiglio non è solo per proteggerti dalla perdita di anonimato ma anche dall'hacking. È meglio non utilizzare mai il laptop Tails dedicato sulla rete Wi-Fi di casa. In questo modo, esso sarà molto meno accessibile a un aggressore remoto rispetto a un computer regolarmente connesso alla rete Wi-Fi di casa. Un aggressore che ti prende di mira ha bisogno di un punto di partenza e la tua rete Wi-Fi domestica è un'ottima base di partenza.
- **Rimuovi il disco rigido**: è più facile di quanto sembri. Se acquisti il laptop, puoi chiedere al negozio di farlo e risparmiare un po' di soldi. Se cerchi su YouTube "rimuovere disco rigido" per il tuo modello specifico di computer, probabilmente troverai un video tutorial. Assicurati di

22 https://www.anarsec.guide/posts/tamper/

rimuovere prima la batteria e di scollegare il cavo di alimentazione. Rimuoviamo il disco rigido per eliminare completamente il firmware del disco stesso, noto per essere vulnerabile agli attacchi hacker. Un disco rigido fa parte della “superficie di attacco” e non è necessario su un sistema live come Tails, che funziona da una chiavetta USB.

- Considera anche di **rimuovere l'interfaccia Bluetooth, la fotocamera e il microfono**, anche se questo è più complicato e richiede il manuale d'uso del tuo modello di laptop. La fotocamera può almeno essere "disabilitata" coprendola con un adesivo. Il microfono è spesso collegato alla scheda madre tramite una spina: in questo caso, basta scollegarlo. Se non è evidente, se il cavo è saldato direttamente alla scheda madre o se il connettore è necessario per altri scopi, taglia il cavo del microfono con un paio di pinze. Lo stesso metodo può essere utilizzato per disattivare definitivamente la fotocamera. È anche possibile utilizzare Tails su un computer "offline" dedicato, rimuovendo la scheda di rete. Alcuni computer portatili hanno degli interruttori sul case che permettono di disattivare le interfacce wireless, ma per un computer offline è preferibile rimuovere effettivamente la scheda di rete.
- **Garantisci l'integrità dell'avvio sostituendo il BIOS con Heads**. Alcuni ricercatori nel campo della sicurezza hanno dimostrato la possibilità di sferrare un attacco al firmware BIOS di un utente Tails, consentendo il furto di chiavi GPG ed e-mail. Purtroppo, a differenza del disco rigido, il BIOS non può essere rimosso. È necessario per accendere il laptop, quindi deve essere sostituito con un firmware open source. Si tratta di un processo avanzato, in quanto richiede l'apertura del computer e l'uso di strumenti speciali. La maggior parte degli utenti non sarà in grado di farlo autonomamente, ma si spera che nella vostra rete ci sia una persona di fiducia che possa configurarlo per voi. Il progetto si chiama "Heads" perché è l'altra faccia di Tails: mentre Tails protegge il software, Heads protegge il firmware. Ha uno scopo simile al Verified Boot presente in GrapheneOS, che stabilisce una catena di fiducia completa dall'hardware. Heads ha una compatibilità limitata, quindi tenetelo a mente quando acquistate il vostro computer, se avete intenzione di installarlo: noi consigliamo il ThinkPad X230, perché è meno complicato da installare rispetto ad altri modelli. Le CPU di questa generazione sono in grado di rimuovere efficacemente l'Intel Management Engine durante il flashing di Heads, ma non è così per le CPU delle generazioni successive presenti nei computer più recenti. Heads può essere configurato per verificare l'integrità e l'autenticità di una USB Tails (vedere la documentazione) e impedire l'avvio se è stata manomessa. Heads protegge da attacchi fisici e remoti al firmware del BIOS e al software del sistema operativo. Se Heads rileva una manomissione, il dispositivo deve essere considerato immediatamente non affidabile. L'analisi forense può rivelare come si è verificata la compromissione e aiutare a prevenire che si ripeta. È possibile contattare un servizio come la Digital Security Helpline di Access Now, anche se si consiglia di non inviare loro dati personali.
- **Utilizza chiavette USB con firmware sicuro,** come Kanguru FlashTrust, che smettono di funzionare se il firmware viene compromesso. Kanguru ha rivenditori in tutto il mondo, il che ti permette di acquistare le chiavette di persona per evitare il rischio di intercettazione della posta.

- **Esegui Tails da una chiavetta USB dotata di interruttore fisico di protezione da scrittura.**

Utilizzo di un interruttore di protezione da scrittura (*write-protect switch*)

Che cos'è un interruttore di *protezione da scrittura*? Quando si inserisce una normale chiavetta USB in un computer, quest'ultimo esegue operazioni di *lettura* e *scrittura* su di essa e un'operazione di *scrittura* può modificare i dati presenti sulla chiavetta. Alcune chiavette USB speciali, sviluppate per l'analisi dei malware†, dispongono di un interruttore fisico che può bloccare la chiavetta, consentendo la *lettura* dei dati, ma impedendo la *scrittura* di nuovi dati.

Se la tua chiavetta USB Tails dispone di un interruttore di protezione da scrittura come il Kanguru FlashTrust, quando l'interruttore è bloccato, sei protetto da un eventuale aggressore che possa compromettere il software Tails memorizzato sulla chiavetta. Questo è fondamentale. Per compromettere la tua chiavetta USB Tails, un aggressore dovrebbe essere in grado di scriverci sopra. Ciò significa che, anche se una sessione Tails viene infettata da malware, la tua chiavetta USB Tails rimane intonsa e la compromissione non può trasferirsi alle sessioni Tails successive ("persistenza del malware") modificando i file del sistema operativo. L'unico altro modo per ottenere la "persistenza del malware" è la compromissione del firmware, che hai già mitigato usando una chiavetta USB con firmware sicuro.

Si noti che il firmware Heads rende superfluo l'interruttore di protezione da scrittura, in quanto può essere configurato per verificare l'integrità e l'autenticità della chiavetta USB Tails prima dell'avvio.

Se non si utilizza Heads e non è possibile ottenere una chiavetta USB con interruttore di protezione da scrittura, sono disponibili tre opzioni.

1. Installa Tails su una scheda SD e utilizza un adattatore da USB 3.0 a scheda SD, in quanto le schede SD dispongono di un interruttore di protezione da scrittura.
2. Masterizza Tails su un nuovo DVD-R o DVD+R (scrivibile una sola volta) per ogni nuova versione di Tails: si tratta di un'operazione piuttosto scomoda. Non utilizzare DVD contrassegnati come "DVD+RW" o "DVD+RAM", che possono essere riscritti.
3. Avvia Tails con l'opzione `"toram"`, che carica Tails completamente nella memoria. Espelli la chiavetta USB Tails all'inizio della sessione, prima di fare qualsiasi altra cosa (che si tratti di connettersi a Internet o di collegare un'altra chiavetta USB), quindi utilizza Tails normalmente. Il modo in cui si utilizza l'opzione "`toram`" dipende dal fatto che la propria USB Tails si avvii con SYSLINUX o GRUB[23].

- Per SYSLINUX, quando appare la schermata di avvio, premi il tasto Tab e digita uno spazio. Digita "toram" e premi Invio.
- Per GRUB, quando appare la schermata di avvio, premi `e` e usa le frecce della tastiera per spostarti alla fine della riga che inizia con `linux`. La riga è probabilmente suddivisa su più righe, ma si tratta di una singola riga di configurazione. Digita `toram` e premi F10 o Ctrl+X.

23 SYSLINUX e GRUB sono diversi *bootloader* utilizzati dalle distribuzioni Linux (cioè quel piccolo programma che si apre subito prima dell'avvio del sistema che ti permette di scegliere cosa far partire), NdT.

Sbloccare l'interruttore

Su una chiavetta USB con interruttore di protezione da scrittura, non sarà possibile apportare modifiche alla chiavetta USB Tails quando l'interruttore è bloccato. Se è possibile apportare modifiche, lo stesso vale per il malware†. Ci sono solo due casi in cui l'interruttore deve essere sbloccato:

1. Per una sessione di aggiornamento dedicata

Se è necessario aggiornare Tails, è possibile farlo in una sessione dedicata con l'interruttore sbloccato, perché l'aggiornamento deve essere scritto sulla chiavetta USB di Tails. Una volta terminato, è necessario riavviare Tails con l'interruttore bloccato.

2. Per una sessione di configurazione dedicata, se si decide di utilizzare l'Archiviazione Persistente

Archiviazione Persistente è una funzione di Tails che consente il trasferimento dei dati tra sessioni altrimenti amnesiche, salvando i dati sulla stessa USB di Tails. Poiché l'Archivio Persistente richiede la scrittura sulla USB di Tails, in genere non è pratico utilizzarlo con un interruttore di protezione da scrittura. Un'alternativa all'interruttore di protezione da scrittura è l'uso di Heads, che verifica l'autenticità e l'integrità della chiavetta USB di Tails tramite una firma digitale all'avvio, garantendo la sicurezza della scrittura sulla chiavetta e consentendo a Persistent Storage di funzionare correttamente.

Un altro motivo per evitare di utilizzare le funzionalità di archiviazione persistente è che molte di esse memorizzano i dati personali sulla chiavetta USB Tails. Se la tua sessione Tails viene compromessa, i dati a cui hai accesso durante quella sessione possono essere utilizzati per ricondurre le tue attività a te. Se sulla chiavetta USB sono presenti dati personali, come un indirizzo di posta elettronica, la compartimentazione delle sessioni Tails *non è più possibile quando l'archiviazione persistente è sbloccata*. Per ottenere la compartimentazione con l'archiviazione persistente sbloccata, è necessario utilizzare una chiavetta USB Tails dedicata per ogni identità e aggiornare tutte le chiavette ogni mese, il che richiederebbe molto lavoro.

Tuttavia, potresti voler utilizzare alcune funzionalità di archiviazione persistente che non memorizzano dati personali, come la funzionalità del software aggiuntivo. Ciò richiede lo sblocco dell'interruttore per una sessione di configurazione dell'archiviazione persistente dedicata.

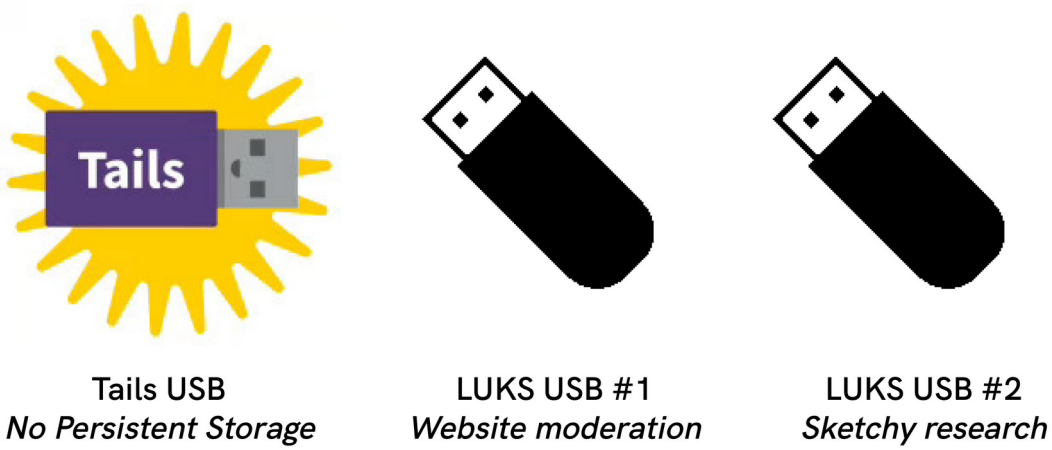
- Avvia una sessione "sbloccata", crea un Archivio Persistente con il software aggiuntivo abilitato, installa il software aggiuntivo e seleziona "Installa ogni volta" quando richiesto.
- Una volta completata la configurazione, riavviare Tails in una sessione "bloccata" prima di utilizzare il software. Non impostare una password di amministrazione, necessaria solo durante l'installazione iniziale. In una sessione "bloccata", nessuno dei file su cui stai lavorando viene salvato sulla chiavetta USB Tails, perché è "bloccata". Tuttavia, il software aggiuntivo è ora configurato per installarsi ogni volta che inserisci la tua password di archiviazione persistente nella schermata di benvenuto. Per ottenere una sessione "bloccata" con Archivio Persistente, l'interruttore USB deve essere impostato su "sola lettura" dopo aver ricevuto la notifica "Software aggiuntivo installato con successo" (prima di connettersi a Internet).

La funzione Archivio Persistente non è disponibile con l'opzione di avvio da DVD o `toram`.

USB "dati personali"

Dove possiamo archiviare i dati personali da utilizzare tra una sessione e l'altra di Tails, se l'interruttore di protezione da scrittura ci impedisce di utilizzare la memoria persistente? Si consiglia di archiviare i dati personali su una seconda chiavetta USB LUKS†. Questa USB "dati personali" non dovrebbe avere lo stesso aspetto della USB Tails per evitare confusione. Se si sta leggendo questo documento da un paese come il Regno Unito, in cui non fornire le password di crittografia può portare al carcere, questa seconda unità dovrebbe essere un HDD contenente un volume nascosto Veracrypt (le unità SSD e USB non sono adatte ai volumi nascosti).

L'approccio di compartimentazione discusso in precedenza separa nettamente le diverse identità utilizzando sessioni Tails separate per attività diverse: ad esempio, nella sessione Tails n. 1 si svolgono attività di moderazione di siti web, mentre nella sessione Tails n. 2 si svolgono attività di ricerca-azione. Questo approccio ha implicazioni sul modo in cui si organizzano le USB "dati personali". Se i file salvati potrebbero essere utilizzati per collegare le vostre attività, è necessario utilizzare una chiavetta USB "dati personali" diversa per ogni attività.



Se si utilizza una chiavetta USB per salvare file molto sensibili, come il testo di un comunicato, è meglio sovrascriverla e poi distruggerla una volta che non se ne ha più bisogno (vedere la sezione "Eliminare definitivamente i dati da una chiavetta USB"). Questo è un altro motivo per utilizzare una chiavetta USB separata per tutti i file che devono essere salvati: in questo modo, non si accumula la cronologia forense di tutti i file sulla memoria persistente di Tails e si possono facilmente distruggere le chiavette USB contenenti i "dati personali" quando necessario.

Se si utilizza già Tails e la posta elettronica crittografata, si potrebbe essere già a conoscenza della funzione Archivio Persistente di Thunderbird per la casella di posta in arrivo e le chiavi PGP. Questa funzione non è compatibile con l'interruttore di protezione da scrittura abilitato. Invece di usare la funzione Archivio Persistente per la posta elettronica, è sufficiente accedere a Thunderbird con IMAP in ogni nuova sessione. Le chiavi PGP† possono essere salvate sull'unità USB "Dati personali" come qualsiasi altro file e importate quando necessario tramite il gestore delle chiavi OpenPGP di Thunderbird (File > Importa chiavi pubbliche da file / Importa chiavi segrete da file). Questo approccio presenta il vantaggio che, anche se le forze dell'ordine riuscissero ad aggirare LUKS†, non avrebbero comunque accesso alla tua casella di posta senza conoscere la tua password di posta elettronica.

Attenzione al phishing

Torniamo al tema di come un avversario potrebbe condurre un attacco remoto contro di voi o il vostro progetto per hackerarlo: la risposta più probabile è il phishing†. Il *phishing* consiste nell'invio di un'e-mail (o di un messaggio in un'applicazione) da parte di un avversario con lo scopo di indurvi a rivelare informazioni o a introdurre malware† nel vostro computer. Lo *spear phishing* si verifica quando l'attaccante ha condotto alcune attività di ricognizione e utilizza le informazioni già in suo possesso su di voi per personalizzare l'attacco di phishing.

Il phishing funziona solo se l'avversario ha un modo per inviarti un messaggio: non devi preoccuparti di questo vettore di attacco per attività come l'invio di un comunicato o la ricerca-azione, ma è rilevante per i progetti rivolti al pubblico che dispongono di un canale di comunicazione. Ricorda che il campo "Da" nelle e-mail può essere falsificato per ingannarti: la firma PGP† mitiga questo rischio, dimostrando che l'e-mail proviene effettivamente da chi ti aspetti.

Probabilmente hai già sentito il consiglio di essere scettico quando clicchi sui link e apri gli allegati: ecco il perché. Il phishing si basa sulle tue azioni per avere successo, quindi la tua consapevolezza è la tua migliore difesa.

Un file o un link dannoso funziona eseguendo del codice sul tuo computer. Nel caso dei file malevoli, il codice viene eseguito quando il file viene aperto. Nel caso dei link malevoli, il codice viene eseguito quando si visita il sito web, solitamente con l'aiuto di JavaScript. Lo scopo dell'esecuzione di questo codice è fornire un punto di accesso ("accesso iniziale") per infettare il tuo computer con malware.

Tails protegge dagli attacchi malware che potrebbero compromettere l'anonimato dell'utente, instradando tutte le connessioni Internet attraverso la rete Tor. Tuttavia, una volta ottenuto l'accesso iniziale, il malintenzionato cercherà di portare avanti il proprio attacco.

- per rendere persistente l'infezione;
- per installare uno screen o un keylogger;
- per sottrarre i dati dell'utente;
- per ottenere un'“escalation dei privilegi”.

L'escalation dei privilegi (ovvero il passaggio da utente senza privilegi a utente amministratore del sistema) è solitamente necessaria per aggirare Tor. Tails non ha una password di amministrazione predefinita (deve essere impostata nella schermata di benvenuto della sessione, se necessario), al fine di rendere più difficile l'escalation dei privilegi.

L'ultimo test di sicurezza di Tails ha rilevato diverse vulnerabilità che consentono l'escalation dei privilegi e persino una di queste che ha divulgato l'indirizzo IP dell'utente senza privilegi. Se la resilienza agli attacchi malware è una parte importante del tuo modello di rischio, consulta “Quando utilizzare Tails vs. Qubes OS”[24].

24 https://www.anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os

File

Nel 2017, l'FBI e Facebook hanno collaborato allo sviluppo di un file video malevolo che ha reso possibile l'identificazione di un utente Tails dopo che questi lo aveva aperto mentre era connesso alla rete Wi-Fi di casa sua.

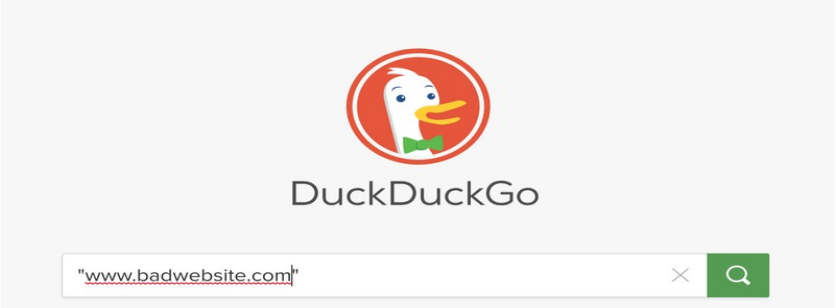
Per gli allegati non attendibili, sarebbe opportuno utilizzare Dangerzone **per ripulire tutti i file prima di aprirli**. Dangerzone trasforma i PDF, i documenti Office o le immagini non attendibili in PDF attendibili. Per sapere come installare Dangerzone su Tails, consulta la documentazione: al momento, è necessario utilizzare la riga di comando.

Se non si utilizza Dangerzone, **è meglio aprire i file non attendibili in una sessione Tails dedicata in "modalità offline"**. Ciò impedirà l'esecuzione del codice di stabilire una connessione remota con l'avversario, solitamente necessaria per portare avanti l'attacco. Chiudere immediatamente la sessione dopo l'apertura ridurrà al minimo la possibilità che il malware persista. Tuttavia, a meno che non si utilizzi Dangerzone per sanificare i file, questi rimarranno non attendibili.

Link

Con i link non affidabili, ci sono due cose che devi proteggere: il tuo anonimato e le tue informazioni.

- **È meglio aprire i link non affidabili in una sessione Tails dedicata, senza Archiviazione Persistente sbloccata o USB con "dati personali" collegate**. Puoi inserire il link su un Riseup Pad per accedervi.
- **Usa Tor Browser con le impostazioni di sicurezza più elevate!** La stragrande maggioranza degli exploit contro Tor Browser non funzionerà con le impostazioni di sicurezza più elevate.
- **Copia e incolla manualmente l'indirizzo nel tuo browser e digita nuovamente il dominio.** Ad esempio, dopo aver incollato il link `anarsec.guide/posts/tails`, digita nuovamente `anarsec.guide`. Non cliccare su un collegamento ipertestuale (copia e incolla sempre), perché potrebbe essere utilizzato per fuorviarti sulla destinazione. Digitare nuovamente il dominio protegge dal "typo-squatting" (che sfruttano errori di battitura, per esempio `mailriseup.net` invece di `mail.riseup.net`) e dagli "attacchi omografici" (in cui le lettere cirilliche sostituiscono quelle normali).
- **Non seguire mai un link abbreviato** (per esempio, un sito come `bit.ly` che prende indirizzi web lunghi e li accorcia) perché non è possibile verificarlo prima del reindirizzamento. `unshorten.me` può rivelare i link abbreviati.
- **Se non riconosci il dominio, effettua una ricerca.** Cerca il dominio tra virgolette utilizzando un motore di ricerca che tutela la privacy (come DuckDuckGo) per verificare che si tratti di un sito web legittimo. Non è una soluzione infallibile, ma è una buona precauzione da adottare.



- **Non inserire alcuna informazione identificativa nel sito web**. Se segui un link contenuto in un'e-mail e ti viene richiesto di effettuare l'accesso, tieni presente che si tratta di una tecnica comunemente utilizzata nelle campagne di phishing. Invece di seguire il link, vai manualmente al sito web del servizio a cui stai cercando di accedere ed effettua il login da lì. In questo modo, saprai di aver effettuato l'accesso al sito web corretto, perché avrai digitato tu stesso l'indirizzo, invece di doverti fidare del link contenuto nell'e-mail.

Attacchi *watering hole*

Un avversario può anche compromettere un sito web "affidabile": questo gli consente di installare malware sui computer di chiunque visiti il sito web senza dover ricorrere al phishing. Questo tipo di attacco è chiamato "watering hole" o "drive-by compromise[25]" perché colpisce molte persone contemporaneamente. Ad esempio, l'FBI ha hackerato un sito web e poi ha utilizzato un exploit del browser Tor[26] per hackerare gli 8.000 utenti che lo hanno visitato.

Ecco perché è importante **utilizzare Tor Browser con le impostazioni di sicurezza più elevate**, anche per i siti web "affidabili", al fine di ridurre notevolmente il rischio di un attacco malware riuscito su Tor Browser.

Crittografia

Password

La crittografia† è l'unica cosa che impedisce ai nostri avversari di leggere tutti i nostri dati, a condizione che venga utilizzata correttamente. Il primo passo per proteggere la crittografia è assicurarsi di utilizzare password molto complesse: la maggior parte delle password non deve essere memorizzata, perché viene archiviata in un gestore di password chiamato KeePassXC; pertanto, può essere completamente casuale. Non riutilizzare mai la stessa password per più scopi ("riciclaggio delle password"): KeePassXC semplifica l'archiviazione di password uniche dedicate a uno scopo specifico. Per imparare a utilizzare KeePassXC, cfr. la sezione dedicata di quest’opuscolo, oppure la pagina web specifica su AnarSec[27].

La crittografia LUKS† è efficace **solo quando il dispositivo è spento**, perché quando è acceso la password può essere recuperata dalla memoria. Gli avversari possono tentare di attaccare la crittografia con un attacco *brute-forcing†*, utilizzando enormi quantità di cloud computing. La versione più recente di LUKS (LUKS2, che utilizza Argon2id) è meno vulnerabile agli attacchi di *brute-forcing†*: questa è l'impostazione predefinita a partire da Tails 6.0 e Qubes OS† 4.1. Se desideri saperne di più su questa modifica, ti consigliamo la panoramica di Systemli[28] o quella di dys2p[29].

La sicurezza di una password si misura in "bit di entropia". Le password/passphrase dovrebbero avere idealmente un'entropia di circa 128 bit (*passphrase diceware* di **dieci parole** o password di **21 caratteri casuali**, inclusi maiuscole, minuscole, numeri e simboli) e non dovrebbero avere un'entropia inferiore a 90 bit (passphrase *diceware* di sette parole).

25 https://attack.mitre.org/techniques/T1189/
26 https://www.vice.com/en/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant
27 https://www.anarsec.guide/posts/tails/#password-manager-keepassxc
28 https://www.systemli.org/en/2023/04/30/is-linux-hard-disk-encryption-hacked/
29 https://dys2p.com/en/2023-05-luks-security.html

Che cos'è una passphrase *diceware* [aleatoria]? Come osserva Privacy Guides, "le passphrase *diceware* sono un'ottima opzione quando è necessario memorizzare o inserire manualmente le proprie credenziali, come la password principale del gestore di password o la password di crittografia del dispositivo. Un esempio di passphrase *diceware* è: "`visibile, resistente, riluttante, morbido, diciassette, mostrato, matita`". La funzione "Password Generator" di KeePassXC può generare passphrase *diceware* e password casuali. Se si preferisce generare passphrase *diceware* utilizzando dadi reali, si consiglia di consultare Privacy Guides[30].

Raccomandazioni generali

- Memorizza passphrase diceware di 7-10 parole per tutto ciò che deve essere inserito prima di avere accesso a un database KeePassXC sbloccato (ovvero la passphrase di crittografia completa del disco e la passphrase master di KeePassXC);
- Genera password casuali di 21 caratteri per tutto ciò che può essere memorizzato in un database KeePassXC. Effettua il backup dei tuoi database KeePassXC in un luogo diverso da quello in cui si trovano i database stessi, nel caso in cui vengano danneggiati o sequestrati.

Suggerimento:

Le passphrase memorizzate con il metodo diceware possono essere facili da dimenticare, soprattutto se ne avete diverse da ricordare, specialmente se le utilizzate raramente. Per ridurre il rischio di dimenticare definitivamente una passphrase diceware, potete utilizzare Tails per memorizzare tutte le passphrase su una chiavetta USB LUKS e conservarla fuori sede, in modo che non possa essere recuperata in caso di irruzione della polizia. Dovresti essere in grado di ricostruire la passphrase LUKS di questa chiavetta USB anche se è passato molto tempo. Ci sono ad es. due diversi approcci che puoi adottare: uno si basa su un* compagn* fidato, l'altro è autosufficiente[31]. Come per tutti i backup importanti, è consigliabile averne almeno due.

Passphrase di Tails

Per Tails, devi memorizzare due passphrase:

1. La passphrase USB LUKS "dati personali", dove è memorizzato il file KeePassXC.
2. La passphrase di KeePassXC.

Se utilizzi l'Archivio Persistente dovrai inserire un'altra passphrase nella schermata di benvenuto all'avvio, ma può essere la stessa della password LUKS. Spegni Tails ogni volta che ti allontani dal computer per più di qualche minuto.

Volumi crittografati

LUKS† è ottimo, ma una difesa approfondita non guasta. Se la polizia sequestra la tua chiavetta USB durante una perquisizione domiciliare, proverà una serie di tattiche per aggirare l'autenticazione; pertanto, un secondo livello di difesa con un'implementazione di crittografia diversa può rivelarsi utile per i dati altamente sensibili.

30 https://www.privacyguides.org/en/basics/passwords-overview/#diceware-passphrases
31 https://www.notrace.how/threat-library/mitigations/digital-best-practices.html#header-use-strong-passwords

Installazione di SiriKali

SiriKali è un programma di crittografia dei volumi che utilizza Gocryptfs in background. È disponibile nel repository Debian e può essere installato facilmente come software aggiuntivo. In Synaptic, installa sia SiriKali che Gocryptfs (se hai dimestichezza con la riga di comando del terminale, puoi usare direttamente Gocryptfs e non hai effettivamente bisogno di SiriKali). Se non si desidera reinstallare SiriKali ad ogni sessione, sarà necessario configurare il software aggiuntivo in Archivio Persistente.

Creazione di un volume crittografato

L'utilizzo di SiriKali per creare il volume genererà due nuove directory: una directory "cipher" in cui verranno archiviati i file crittografati (VolumeName/ sulla tua USB "dati personali") e una directory "plain" in cui potrai accedere al volume una volta che sarà stato montato (/home/amnesia/.SiriKali/VolumeName).

- Collegare la chiavetta USB "Dati personali" in cui verrà memorizzato il volume crittografato e inserire la passphrase LUKS.
- Quindi, in SiriKali, premere "Crea volume" e selezionare l'opzione "gocryptfs".
- Verrà richiesta una password. Creare una nuova voce nel file KeepassXC e generare una password utilizzando la funzione "Genera password" (icona del dado).
- Per l'opzione "Volume Path" (Percorso volume), seleziona la chiavetta USB "Dati personali" che hai appena sbloccato.

Accesso al volume crittografato

Ogni volta che si desidera decrittare il volume, fare clic su "Monta volume".

- Questo avviene automaticamente al momento della creazione del volume.
- A questo punto, puoi aggiungere file al volume montato facendo clic con il tasto destro del mouse sul volume e selezionando "Apri cartella".
- Puoi verificare che SiriKali funzioni creando un file di prova in questa cartella. Questo file apparirà crittografato nella directory Cipher.
- Quando hai finito, fai clic con il tasto destro del mouse sul volume e seleziona "Smonta".

Prima di archiviare file importanti nel volume, ti consigliamo di eseguire un test per assicurarti che funzioni correttamente, soprattutto se lo usi per la prima volta.

Comunicazione crittografata

L'e-mail PGP è la forma più consolidata di comunicazione crittografata su Tails nell’ambiente anarchico. Purtroppo, PGP non garantisce la segretezza diretta: un singolo segreto (la chiave privata) può decifrare tutti i messaggi, non solo uno, come invece avviene nella messaggistica crittografata odierna. È l'opposto della "protezione dei metadati" e presenta diversi altri difetti[32].

Per la messaggistica *sincrona†* e *asincrona†* consigliamo Cwtch[33], a meno che non si tratti di un progetto pubblico anonimo, nel qual caso consigliamo comunque PGP. Per ulteriori informazioni, consultare la guida Messaggistica crittografata per anarchici[34].

32 https://www.anarsec.guide/posts/e2ee/#pgp-email
33 https://www.anarsec.guide/posts/e2ee/#cwtch
34 https://www.anarsec.guide/posts/e2ee/

Per concludere

L'uso di Tails senza seguire questi consigli rappresenta comunque un notevole miglioramento rispetto a molte altre opzioni. Dato che gli anarchici affidano regolarmente la propria libertà a Tails, adottare queste ulteriori precauzioni può rafforzare ulteriormente la fiducia in questo sistema operativo.

Appendice : Come rimuovere i metadati identificativi dai file

I metadati sono *dati sui dati* o *informazioni sulle informazioni*. Nel contesto dei file, i metadati possono essere informazioni incorporate automaticamente nel file stesso e utilizzabili per identificare il file. Ad esempio, un file immagine può contenere metadati relativi alla data e al luogo in cui è stata scattata la foto, nonché al modello di fotocamera utilizzato. Un file PDF, per esempio, può contenere informazioni sul programma con cui è stato creato, sul computer utilizzato, ecc. Queste informazioni possono essere utilizzate dagli investigatori per collegare una foto alla fotocamera con cui è stata scattata, un video al computer su cui è stato modificato, e così via. Prima di pubblicare un file sensibile su Internet, è necessario rimuovere i metadati.

Strumenti per rendere anonimi metadati

Fortunatamente, esiste uno strumento che pulisce completamente i metadati e che è disponibile sia come interfaccia a riga di comando che come interfaccia grafica. La versione a riga di comando si chiama `mat2` ed è open source, mentre la versione grafica si chiama Metadata Cleaner ed è anch'essa open source. Entrambi i programmi sono inclusi di default in Tails e Qubes†-Whonix.

Utilizzo di Metadata Cleaner

Se non avete familiarità con la riga di comando, vi consigliamo di utilizzare Metadata Cleaner, che utilizza `mat2` come motore, quindi offre le stesse funzionalità. Metadata Cleaner è migliore di Exiftool e di altri software per la rimozione dei metadati: consultate i documenti di confronto[35].

Metadata Cleaner mostra i metadati rilevati, ma "il fatto che Mat2 non ne mostri nessuno non significa che un file sia privo di metadati. Non esiste un metodo affidabile per rilevare tutti i possibili metadati per i formati di file complessi". Ciò significa che è necessario pulire il file anche se non vengono visualizzati i metadati.

Per utilizzare Metadata Cleaner, aggiungi prima un file. Fai clic sul file e verranno visualizzati i metadati correnti. Seleziona il file e poi seleziona "**Pulisci"**. Per verificare che i metadati siano stati rimossi, aggiungi nuovamente il file pulito e visualizzane i metadati.

Quando si pulisce un file PDF, questo viene convertito in immagini, pertanto la qualità viene ridotta e non è possibile selezionare il testo al suo interno. Se si desidera mantenere questa possibilità, è disponibile una modalità di pulizia *leggera* che pulisce solo i metadati superficiali del file, ma non quelli delle "risorse incorporate" (come le immagini nel PDF). Se si sta creando un PDF, è consigliabile utilizzare Metadata Cleaner su tutte le immagini prima di importarle nel software di impaginazione e utilizzare un software di impaginazione generico per quei sistemi operativi, come Scribus, su Tails o Qubes-Whonix. È possibile abilitare la "pulizia leggera" nelle impostazioni di Metadata Cleaner.

35 https://0xacab.org/jvoisin/mat2/-/blob/master/doc/comparison_to_others.md

Tieni presente che Metadata Cleaner ha le seguenti limitazioni: "mat2 rimuove solo i metadati dai tuoi file, non rende anonimo il loro contenuto e non è in grado di gestire filigrane, steganografia o qualsiasi campo/sistema di metadati troppo personalizzato. Se si desidera davvero essere anonimi, è consigliabile utilizzare formati di file che non contengono metadati o, meglio ancora, il testo semplice".

Analisi forensi di foto e video

Sebbene sia possibile rimuovere tutti i metadati da un'immagine o da un video, l'analisi forense può comunque rivelare il dispositivo utilizzato per acquisirli. Come indicato nella documentazione di Whonix:

Ogni sensore di una fotocamera presenta una firma di rumore unica a causa di sottili differenze hardware. Il rumore del sensore è rilevabile nei pixel di ogni immagine e video ripresi con la fotocamera e può essere identificato come un'impronta digitale. Allo stesso modo in cui la balistica forense può risalire alla canna da cui proviene un proiettile, la digital forensics può risalire al dispositivo utilizzato per acquisire immagini e video. Si noti che questo effetto è diverso dai metadati dei file.

In questo modo, è possibile collegare tra loro più foto o video provenienti dalla stessa fotocamera e, se la fotocamera viene recuperata, è possibile confermare l'origine dei file. È possibile acquistare fotocamere economiche da un banco dei pegni e utilizzarle una sola volta per scattare foto o registrare video che richiedono un elevato livello di sicurezza.

Analisi forensi delle stampanti

Tutte le stampanti moderne lasciano filigrane invisibili che codificano informazioni quali il numero di serie della stampante e la data di stampa. Quando il materiale stampato viene scansionato, questi segni sono presenti nel file. Per ulteriori informazioni, consultare i documenti *Rivelare tracce nelle stampe e nelle scansioni*[36] e Whonix sulla stampa e la scansione[37].

Glossario

Asincrona [comunicazione]

A differenza della comunicazione sincrona, in questo caso non è necessario che entrambe le parti siano online contemporaneamente. Questo tipo di comunicazione si basa su un server che memorizza i messaggi fino a quando i destinatari non si connettono. Si tratta del tipo di messaggistica più diffuso (e-mail, ecc.).

Attacco di correlazione

Un attacco di correlazione è un metodo sofisticato usato da attori malintenzionati per compromettere l’anonimato dell’utente della rete, in particolare di quella Tor. Il concetto fondamentale è quello dell’analisi dei pattern del traffico per collegare l’attività virtuale dell’utente alla sua identità nel mondo reale. L’avversario che esegue questo tipo di attacchi solitamente lo fa da un punto avvantaggiato dall’accesso contemporaneo ai nodi di entrata e di uscita della rete Tor: monitorando il traffico in entrata e uscita può così correlare il comportamento dell’utente. Questa sincronizzazione consente la potenziale

36 https://dys2p.com/en/2022-09-print-scan-traces.html
37 https://www.whonix.org/wiki/Printing_and_Scanning

compromissione dell’anonimato di utenti Tor, poiché l’attaccante può tracciare le informazioni fino alla fonte.

Un attacco di correlazione *end-to-end* esemplifica la tecnica prevalente di questo tipo di attacchi. In questo scenario, l’avversario cattura sufficienti pacchetti di dati da entrambi i lati (nodi) per accertare la probabilità di una correlazione tra il traffico in entrata e in uscita, sfruttando i pattern di forma (*bandwith*) e di tempistica del flusso di dati.

Nessuna rete di anonimato utilizzata per connessioni rapide (web o messaggistica istantanea) è immune al 100% da questo tipo di attacchi. Le VPN (Virtual Private Network) ad es., sono meno sicure di Tor perché non utilizzano 3 relay indipendenti.

Attacco DDoS

Un attacco Distributed Denial of Service (DDoS) tenta di sovraccaricare o bloccare i servizi di un sistema inviando un numero elevato di richieste da molte fonti. L'obiettivo di un attacco DDoS è compromettere la disponibilità di un servizio o di un sistema, ad esempio rendendo un server web non raggiungibile dai browser.

Attacchi fisici

Un attacco fisico si verifica quando un avversario ottiene l'accesso fisico al dispositivo dell'utente tramite smarrimento, furto o confisca. Ad esempio, il telefono potrebbe essere sequestrato quando si attraversa un confine o si viene arrestati. Ciò è in contrasto con un attacco remoto.

Attacco *man-in-the-middle*

Un esempio di attacco *man-in-the-middle* si verifica quando Tizia comunica con Caio su Internet e DigosBoia (l'intercettatore) si unisce alla conversazione "nel mezzo", diventando il *man-in-the-middle*. DigosBoia può modificare, inserire, riprodurre o leggere i messaggi a suo piacimento. Le misure di protezione includono la crittografia (per garantire la riservatezza) e la verifica dell'autenticità e dell'integrità di tutti i messaggi. Tuttavia, è necessario anche assicurarsi di comunicare con la parte prevista. È necessario verificare di avere la chiave pubblica reale del destinatario. Ad esempio, questo è ciò che si fa quando si verifica il "numero di sicurezza" di un contatto nell'app di messaggistica crittografata Signal.

Attacchi remoti

Per attacco remoto s'intende l'accesso da parte di un malintenzionato ai dati presenti su un telefono o un laptop tramite una connessione Internet o dati. Esistono aziende che sviluppano e vendono la possibilità di infettare il dispositivo (solitamente uno smartphone) con un malware che consentirebbe al loro cliente (un malintenzionato, che si tratti di un'azienda o di un agente statale) di accedere in remoto a parte o a tutte le informazioni. Ciò è in contrasto con un attacco fisico.

Autenticazione a due fattori (2FA)

L'autenticazione a due fattori (o 2FA) è un metodo di identificazione di un utente presso un fornitore di servizi che richiede una combinazione di due diversi metodi di autenticazione. Questi possono essere qualcosa che l'utente conosce, come una password o un PIN, o qualcosa che l'utente possiede, come un token hardware o un telefono cellulare.

Backdoor

Una backdoor nel software o nell'hardware consente a un soggetto non autorizzato di aggirare i controlli di accesso. Ad esempio, un account sviluppatore non documentato in un router consente allo sviluppatore del prodotto di aggirare il modulo di accesso. Anche le terze parti possono utilizzare le backdoor per accedere ai software/hardware. Gli hacker vogliono creare backdoor, così come le forze dell'ordine.

Brute-forcing

Un aggressore che "semplicemente" prova tutte le chiavi possibili per accedere a un servizio o decriptare un file sta utilizzando la "forza bruta". Questo processo è chiamato "attacco di brute-forcing". I computer più potenti rendono gli attacchi brute-forcing più fattibili. I moderni protocolli crittografici sono progettati per costringere un avversario (che non possiede la chiave crittografica) a impiegare quasi tutto il tempo necessario per provare tutte le possibili chiavi di decodifica. I parametri di un buon protocollo sono scelti in modo da rendere impraticabile questo lasso di tempo.

Checksum/impronte digitali

I checksum sono impronte digitali, ovvero piccoli blocchi di dati derivati da un altro blocco di dati digitali, utilizzati per rilevare eventuali modifiche apportate. Ad esempio, quando si scarica un file ISO del sistema operativo, viene visualizzato un checksum simile a: SHA512: 9f923361887ac4b1455bc5ae51c06f2457c6d (continua...). È possibile utilizzare funzioni hash come SHA512 per creare impronte digitali. In pratica, questa operazione matematica converte gli 0 e gli 1 del file in un'impronta digitale unica. La modifica di un solo 1 o 0 comporta un'impronta digitale completamente diversa. Spesso è importante sapere se un file è stato modificato, ad esempio quando si scarica l'immagine di un sistema operativo. Le impronte digitali sono spesso utilizzate in ambito crittografico, ad esempio nei certificati o per verificare le chiavi pubbliche in generale. GtkHash è un programma che consente di calcolare i checksum senza utilizzare un'interfaccia a riga di comando.

Crittografia

La crittografia è il processo di codifica di un messaggio in modo che possa essere decodificato (e letto) solo dalle parti interessate. Il metodo utilizzato per codificare il messaggio originale, o testo in chiaro, è chiamato cifrario o protocollo di crittografia. In quasi tutti i casi, il cifrario non è destinato a rimanere segreto. Il messaggio codificato, illeggibile e crittografato, è chiamato "testo cifrato" e può essere condiviso in modo sicuro. La maggior parte dei cifrari richiede un'ulteriore informazione, chiamata chiave crittografica, per crittografare e decrittare i messaggi.

I dati vengono crittografati mentre viaggiano da un dispositivo all'altro, da un punto all'altro, e non possono essere decifrati da alcun intermediario bensì solo dagli *endpoint*. Ciò è diverso dalla "crittografia

a riposo", come la crittografia completa del disco, in cui i dati memorizzati sul dispositivo vengono crittografati quando il dispositivo è spento. Entrambe sono importanti!

Crittografia a chiave pubblica

La crittografia a chiave pubblica (o asimmetrica) è l'opposto della crittografia simmetrica. Ogni parte dispone di due chiavi: una pubblica e una privata. La chiave privata deve essere mantenuta segreta e viene utilizzata per la decrittazione, mentre la chiave pubblica deve essere resa pubblica e viene utilizzata per la crittografia. Questo modello viene utilizzato per la comunicazione crittografata, in quanto la chiave pubblica non può essere impiegata per la decrittazione. Tutte le altre parti devono verificare che la chiave pubblica pubblicata appartenga al proprietario previsto, al fine di evitare attacchi man-in-the-middle.

Esistono diversi approcci alla crittografia a chiave pubblica. Ad esempio, alcuni sistemi crittografici si basano sulla struttura algebrica delle curve ellittiche su campi finiti (ECC). Altri ancora si basano sulla difficoltà di scomporre il prodotto di due grandi numeri primi (RSA). La crittografia a chiave pubblica può essere utilizzata anche per le firme digitali.

Crittografia completa del disco (FDE)

FDE significa che l'intero disco è crittografato fino all'inserimento della password all'accensione del dispositivo. Non tutte le FDE sono uguali. Ad esempio, la qualità dell'implementazione della FDE su un telefono dipende non solo dal sistema operativo, ma anche dall'hardware (il modello del telefono). La FDE utilizza la crittografia simmetrica e, su Linux, utilizza generalmente la specifica LUKS.

Crittografia simmetrica

La crittografia simmetrica è l'opposto della crittografia a chiave pubblica. Due parti hanno bisogno della stessa chiave privata per comunicare tra loro. Entrambe le parti utilizzano la stessa chiave per crittografare e decrittare i dati. La crittografia simmetrica è più veloce di quella a chiave pubblica, ma è necessario scambiare le chiavi in modo sicuro. AES è un noto esempio di crittografia simmetrica. Questo modello viene utilizzato per la crittografia completa del disco (ad esempio, da LUKS nella crittografia completa del disco Linux).

Doxxing

La pubblicazione di informazioni private su un individuo o un'organizzazione è chiamata "doxxing". Prima della pubblicazione, la persona che effettua il doxxing può utilizzare database pubblici, social media o ingegneria sociale per ottenere le informazioni desiderate.

Exploit

Un exploit è progettato per sfruttare una vulnerabilità. Ancora peggiori (o migliori, a seconda che tu sia l'aggressore o la vittima) sono gli exploit zero-day.

Exploit zero-day

Un exploit zero-day è sconosciuto al pubblico, al fornitore o ad altre parti che normalmente lo mitigherebbero. Di conseguenza, è estremamente potente e molto ambito. I governi possono sviluppare i propri exploit zero-day o acquistarli da un fornitore specializzato.

Firme digitali

Le firme digitali si basano sulla crittografia a chiave pubblica. Una chiave privata viene utilizzata per firmare digitalmente i dati, mentre la chiave pubblica corrispondente viene impiegata da terzi per verificarne l'autenticità. Prima di utilizzare una chiave pubblica per verificare una firma, è necessario verificarne l'autenticità.

Forward secrecy

La forward secrecy (FS, nota anche come "Perfect Forward Secrecy") combina un sistema di chiavi a lungo termine e chiavi di sessione per proteggere le comunicazioni crittografate da future compromissioni delle chiavi. Un aggressore in grado di registrare ogni messaggio crittografato (man-in-the-middle) non potrà decrittare tali messaggi se le chiavi dovessero essere compromesse in futuro. I moderni protocolli di crittografia, come TLS 1.3 e il protocollo Signal, forniscono la FS.

GnuPG/OpenPGP

GnuPG (PGP) è un programma che implementa lo standard OpenPGP (Pretty Good Privacy). PGP fornisce funzioni crittografiche per crittografare, decrittare e firmare testi e file. Si tratta di un classico esempio di crittografia a chiave pubblica. Quando viene utilizzato con la posta elettronica, i metadati (come gli indirizzi e-mail) rimangono non crittografati. Non garantisce la segretezza diretta.

HTTPS

La "S" in HTTPS sta per "sicuro"; ciò significa che la tua connessione Internet è crittografata utilizzando il protocollo Transport Layer Security (TLS). Ciò comporta la generazione, da parte del sito web, di un certificato che utilizza la crittografia a chiave pubblica e che può essere utilizzato per verificarne l'autenticità, ovvero per accertare che ti stai effettivamente connettendo al server web desiderato e che la connessione è crittografata.

Ingegneria sociale

L'ingegneria sociale è un termine generico che indica la manipolazione psicologica delle persone per indurle a compiere determinate azioni. L'ingegneria sociale non dipende dalla tecnologia ed è piuttosto comune nella vita di tutti i giorni. Ad esempio, i bambini piangono per manipolare i genitori e gli spot pubblicitari manipolano gli spettatori. Nell'ambito della sicurezza informatica, il phishing è una tecnica di ingegneria sociale molto diffusa.

Interfaccia a riga di comando (CLI)

La "riga di comando" è un'alternativa testuale allo strumento grafico "punta e clicca" con cui la maggior parte di noi è più familiare; l'interfaccia a riga di comando (CLI) ci permette di fare alcune cose che un'interfaccia grafica utente (GUI) non consente. Spesso, sia una GUI che una CLI funzionano e la scelta dipende dalle preferenze personali. Ad esempio, in Tails, è possibile verificare il checksum di un file utilizzando il programma GtkHash (GUI) o il comando sha256sum (CLI).

Linux

Linux è un *kernel* [componente centrale di un sistema operativo che fa da ponte tra hardware e software] open source su cui sono costruiti i vari sistemi operativi. A differenza di Windows o macOS, esistono molte varianti di sistemi operativi Linux. Ad esempio, Ubuntu, Kali e Tails sono basati su Debian. Manjaro, invece, si basa su Arch.

LUKS

Il Linux Unified Key Setup (LUKS) è una specifica indipendente dalla piattaforma per la crittografia dei dischi. Si tratta dello standard utilizzato in Tails, Qubes OS, Ubuntu e altri sistemi operativi. La crittografia LUKS è efficace solo quando il dispositivo è spento. LUKS dovrebbe utilizzare Argon2id per renderlo meno vulnerabile agli attacchi brute-forcing.

Malware

Il termine "malware" (software dannoso) indica un software che contiene funzionalità indesiderate o dannose. Il malware include ransomware, cavalli di Troia, virus informatici, worm, spyware, scareware, adware, ecc. Oggi, il malware è più difficile da classificare perché, nella sua versione più sofisticata, spesso combina caratteristiche di diverse categorie. Ad esempio, WannaCry si è diffuso come un worm, ma ha anche crittografato i file e li ha tenuti in ostaggio (ransomware).

Metadati

I metadati sono dati che forniscono informazioni su altri dati. Ad esempio, un file JPG contiene l'immagine effettiva (i dati), ma può anche contenere metadati quali la data di creazione del file, il tipo di fotocamera utilizzata, le coordinate GPS e così via. I metadati possono essere preziosi per gli hacker (per trovare exploit appropriati per software obsoleti utilizzati dal bersaglio), per le agenzie governative (per raccogliere informazioni sulle persone e creare grafici sociali) e per altre parti interessate (per indirizzare pubblicità basate sulla posizione). Ogni volta che si utilizza un computer, è probabile che si lascino tracce di metadati.

Modello di rischio

L’elaborazione del modello del rischio è un insieme di attività volte a migliorare la sicurezza di un sistema, che prevede l'identificazione di avversari, obiettivi di sicurezza e vulnerabilità, e la definizione di contromisure per prevenire o mitigare gli effetti delle minacce. Una minaccia è un evento indesiderato, potenziale o effettivo, che può essere dannoso (come un attacco DDoS) o accidentale (come un guasto del

disco rigido). Elaborare un modello di rischio consiste nell'identificare e valutare in modo deliberato minacce e vulnerabilità.

Negabilità plausibile

La negabilità plausibile può essere un obiettivo di sicurezza. Si ottiene quando non è possibile dimostrare che una persona o un sistema abbia inviato un determinato messaggio. In tal caso, il mittente può negare in modo plausibile di essere l'autore del messaggio.

Open source

L'unico software di cui possiamo fidarci è quello il cui "codice sorgente" è "aperto", in modo che chiunque possa esaminarlo.

Passphrase

Una passphrase è simile a una password, ma è composta da parole invece che da caratteri casuali.

Password

Una password è una stringa di caratteri utilizzata per l'autenticazione. Una password forte è composta da caratteri scelti in modo casuale, con la stessa probabilità di occorrenza per ciascuno di essi, e può essere creata con il generatore di password di KeePassXC.

Phishing

Il phishing è una tecnica di ingegneria sociale. Gli aggressori inviano messaggi SMS, e-mail, messaggi di chat, ecc. alle loro vittime per ottenere le loro informazioni personali. In questo modo, gli aggressori possono cercare di impersonare le loro vittime. Può anche essere utilizzato per indurre la vittima a scaricare malware su un sistema che può essere utilizzato come punto di partenza per l'hacking. Lo spear phishing è una forma più sofisticata di phishing.

Qubes OS

Qubes OS può essere considerato come una versione di Linux con macchine virtuali. Lo consigliamo come sistema operativo quotidiano per gli utenti Linux di livello intermedio.

Sandboxing

Il sandboxing consiste nell'isolamento basato su software delle applicazioni per mitigare guasti o vulnerabilità del sistema. Ad esempio, se un aggressore hackera un'applicazione "sandboxata", deve uscire dalla sandbox per hackerare l'intero sistema. La virtualizzazione è la forma più potente di sandboxing.

Sincrona [comunicazione]

A differenza della comunicazione *asincrona*, in questo caso entrambe le parti devono essere online contemporaneamente. Questo tipo di comunicazione non richiede server e viene spesso definito "peer to peer".

Sistema operativo (OS)

Si tratta del software di sistema che gestisce il dispositivo prima di qualsiasi altro software. Alcuni esempi comuni sono Windows, macOS, Linux, Android e iOS. Linux e alcune versioni di Android sono le uniche opzioni open source presenti in questo elenco.

Spear phishing

Lo spear phishing è più sofisticato del phishing tradizionale, che getta una rete più ampia. In questo caso, gli aggressori personalizzano i loro messaggi contraffatti e li inviano a un numero più ristretto di potenziali vittime. Questo tipo di attacco richiede una maggiore ricerca da parte dell'aggressore, ma il tasso di successo degli attacchi di spear phishing è superiore a quello degli attacchi di phishing tradizionali.

Tails

Tails è un sistema operativo che rende l'uso sicuro e anonimo del computer accessibile a tutti. Tails funziona da un'unità USB ed è progettato per non lasciare tracce della tua attività sul computer, a meno che tu non lo desideri esplicitamente.

Tails utilizza la rete anonima Tor per proteggere la privacy online e tutto il software è configurato per connettersi a Internet tramite Tor. Se un'applicazione tenta di connettersi direttamente a Internet, viene automaticamente bloccata per motivi di sicurezza.

Tor Network

Tor (abbreviazione di The Onion Router) è una rete aperta e distribuita che aiuta a difendersi dall'analisi del traffico. Tor protegge le tue comunicazioni instradandole attraverso una rete di relay gestiti da volontari in tutto il mondo e impedisce agli operatori dei siti che visiti di conoscere la tua posizione fisica.

Ogni sito web visitato attraverso la rete Tor passa attraverso tre relay. I relay sono server ospitati da persone e organizzazioni di tutto il mondo. Nessun relay conosce né la provenienza né la destinazione della connessione crittografata. Un estratto da una valutazione top secret della NSA, trapelato, definisce Tor "il re dell'anonimato su Internet ad alta sicurezza e bassa latenza", senza "alcun contendente al trono in attesa". È possibile accedere alla rete Tor tramite il browser Tor su qualsiasi sistema operativo. Il sistema operativo Tails obbliga ogni programma a utilizzare la rete Tor quando accede a Internet.

Virtualizzazione

La virtualizzazione è una tecnologia che crea una versione virtuale di qualcosa, incluso l'hardware di un computer. Una macchina virtuale sfrutta questa tecnologia.

- **Macchina virtuale (VM)**

  Una macchina virtuale è una virtualizzazione/emulazione di un sistema informatico. Le macchine virtuali si basano su architetture informatiche e forniscono le funzionalità di un computer fisico. Ciò offre il vantaggio di poter utilizzare il sandboxing in termini di sicurezza. Qubes OS è costituito da macchine virtuali che funzionano direttamente sull'hardware (denominato "bare metal"). Secondo il progetto Qubes, "la virtualizzazione è attualmente l'unico approccio praticamente praticabile per implementare un forte isolamento e garantire al contempo la compatibilità con le applicazioni e i driver esistenti".

VoIP (Voice over Internet Protocol)

Google Voice è un noto servizio VoIP che non è sicuro; questa tecnologia instrada le chiamate su Internet, come fa Signal, invece di utilizzare la trasmissione standard tramite ripetitori cellulari. A differenza di Signal, il VoIP consente di ricevere chiamate da chiunque, non solo da altri utenti Signal. Il vantaggio di utilizzare il VoIP con un piano dati è che è possibile creare numeri diversi per attività diverse (uno per le bollette, uno per la registrazione di un account Signal, ecc.) e non è mai necessario attivare la modalità aereo. Il vantaggio di utilizzare un piano dati è che puoi utilizzarlo anche lontano dal Wi-Fi, a costo però della geolocalizzazione (ovvero, il tuo fornitore di servizi e potenzialmente altre parti potranno sapere dove si trova il tuo dispositivo in un dato momento).

VPN (rete privata virtuale)

Una VPN estende una rete privata (come quella domestica) su una rete pubblica (come Internet). I dispositivi connessi alla VPN fanno parte della rete privata, anche se si trovano fisicamente altrove. Le applicazioni che utilizzano una VPN sono soggette alle funzionalità, alla sicurezza e alla gestione della rete privata.

In altre parole, si tratta di una tecnologia che fa sembrare che ti stai connettendo a Internet dalla rete dell'azienda che fornisce il servizio piuttosto che dalla tua rete domestica. La connessione all'azienda avviene attraverso un "tunnel" crittografato. Una VPN non è lo strumento migliore per garantire l'anonimato (definito come la possibilità di non essere identificati - Tor è molto meglio), ma può migliorare parzialmente la privacy (definita come la possibilità di non essere tracciati).

È importante sottolineare questo aspetto per sfatare il clamore pubblicitario diffuso: una VPN non garantisce l'anonimato. L'uso di una VPN può essere considerato semplicemente come uno spostamento della fiducia da un provider di servizi Internet locale, che è noto per essere un informatore, a un'azienda remota che dichiara di limitare la propria capacità di spiare efficacemente l'utente.

Vulnerabilità

Le vulnerabilità sono falle di sicurezza che possono essere sfruttate nel software o nell'hardware. Le vulnerabilità più note hanno nomi come Heartbleed, Shellshock, Spectre o Stagefright e almeno un identificatore CVE (Common Vulnerabilities and Exposures). Non tutte le vulnerabilità hanno un exploit. Un sistema di classificazione molto diffuso per la gravità delle vulnerabilità è il CVSS.

Tails è un sistema operativo che rende accessibile a tutt un utilizzo sicuro e anonimo del computer . Tails funziona da un'unità USB ed è progettato per non lasciare tracce della tua attività sul computer, a meno che tu non lo desideri esplicitamente.*