OnionShare: Come Condividere File in Modo Anonimo e Sicuro tramite Tor

Maria Cattini | 28/01/2026 | Open source intelligence

Un'indagine OSINT richiede discrezione. Un caso di cybersecurity ancora di più. Quando invii documenti riservati tramite WeTransfer o Google Drive, lasci tracce digitali: il tuo IP, quello del destinatario, metadati della transazione. Ogni passaggio viene registrato. La domanda è semplice: ti fidi davvero di questi servizi quando gestisci materiale sensibile?

OnionShare risolve questo problema. Si tratta di uno strumento open source del Tor Project che cripta e anonimizza il trasferimento di file, senza intermediari e senza lasciare briciole digitali. I dati partono direttamente dal tuo computer, attraversano la rete Tor e arrivano al destinatario senza passare da server esterni.

Cos'è OnionShare e Come Funziona

OnionShare trasforma il tuo computer in un server web temporaneo accessibile solo attraverso la rete Tor. Quando carichi un file, il programma genera un indirizzo .onion univoco: una stringa alfanumerica che funge da chiave d'accesso. Solo chi possiede questo link può scaricare i dati.

Il meccanismo è diretto. I file non vengono caricati su cloud o piattaforme terze. Rimangono sul tuo disco rigido. OnionShare crea un tunnel criptato che collega il tuo dispositivo a quello del destinatario, passando attraverso i nodi della rete Tor. Ogni connessione viene instradata attraverso tre livelli di crittografia (da qui il nome "onion", cipolla), rendendo impossibile risalire alla sorgente.

Perché la Rete Tor Garantisce l'Anonimato

Tor maschera la tua identità frammentando la connessione attraverso relay sparsi nel mondo. Nessun nodo conosce l'intero percorso: il primo sa chi sei ma non dove vai, l'ultimo sa dove vai ma non chi sei. Nel mezzo, tutto è criptato.

Questo rende OnionShare ideale per giornalisti che ricevono documenti riservati, ricercatori OSINT che scambiano prove digitali, o professionisti della sicurezza informatica che devono trasferire log di sistema senza esporsi.

Come Installare OnionShare: Procedura Passo-Passo

La configurazione richiede pochi minuti. Prima serve il browser Tor, scaricabile da torproject.org. Senza questo, il destinatario non potrà accedere ai file.

Fase 1: Download e Installazione

Vai su onionshare.org e seleziona il tuo sistema operativo. Il software supporta Windows, macOS e diverse distribuzioni Linux (Ubuntu, Fedora, Debian). Il file pesa circa 50 MB. Dopo il download, esegui l'installer. Su Windows, clicca due volte sul file .exe e segui le istruzioni. Su Linux, apri il terminale e digita i comandi indicati sul sito ufficiale.

Fase 2: Primo Avvio e Connessione a Tor

Apri OnionShare. Una barra di caricamento mostra la connessione alla rete Tor. Il processo dura 10-30 secondi, a seconda della velocità della tua connessione. Quando appare l'interfaccia principale, sei pronto.

L'interfaccia ha tre schede: "Condividi file", "Ricevi file", "Pubblica sito web". Ogni modalità ha uno scopo specifico.

Inviare File con OnionShare: Guida Pratica

Supponiamo di dover inviare un report di analisi forense digitale a un collega. Il documento contiene screenshot di attività sospette e non può transitare su canali non sicuri.

Step 1: Seleziona i File

Vai alla scheda "Condividi file". Trascina il documento nell'area centrale oppure clicca su "Aggiungi" e selezionalo manualmente. OnionShare accetta qualsiasi formato: PDF, immagini, video, archivi compressi. Non ci sono limiti di dimensione, ma file molto grandi richiedono più tempo per il download.

Step 2: Avvia il Server

Clicca su "Inizia condivisione". OnionShare genera un indirizzo .onion, una stringa simile a questa:

http://4acth47i6kxnvkewtm6q7ib2s3ufpo5sqbsnzjpbi7utijcltosqemad.onion/

Questo link è temporaneo e unico. Copialo e invialo al destinatario attraverso un canale criptato (Signal, ProtonMail, Session).

Step 3: Il Destinatario Scarica i Dati

Chi riceve il link deve aprirlo nel browser Tor. Apparirà una pagina minimalista con il pulsante "Scarica file". Cliccando, parte il download. Al termine, OnionShare chiude automaticamente la connessione e cancella il link. Nessuno potrà più accedere a quei dati.

Modalità Pubblico: Condividere con Più Persone

Di default, OnionShare distrugge il link dopo il primo download. Se devi inviare lo stesso file a più destinatari, attiva la "Modalità pubblico" nelle impostazioni (icona ingranaggio in alto a destra). Il link rimarrà valido finché non interrompi manualmente la condivisione.

Attenzione: questa opzione riduce la sicurezza. Chiunque intercetti il link può accedere ai file. Usala solo quando necessario.

Ricevere File in Modo Anonimo

Rovesciamo lo scenario. Stai conducendo un'indagine OSINT e una fonte vuole inviarti documenti riservati, ma non ha OnionShare installato. Nessun problema.

Step 1: Attiva la Modalità Ricezione

Clicca sulla scheda "Ricevi file". Premi "Avvia modalità ricezione". OnionShare genera un nuovo indirizzo .onion.

Step 2: Condividi il Link

Invia questo indirizzo alla tua fonte. Non serve che installi nulla: basta il browser Tor.

Step 3: Caricamento Remoto

La fonte apre il link nel browser Tor, seleziona i file dal proprio computer e clicca su "Invia file". I dati vengono caricati direttamente sul tuo dispositivo, criptati durante il transito.

OnionShare mostra una notifica quando ricevi nuovi file. Puoi visualizzare la lista cliccando sulla freccia in alto a destra.

Pubblicare Siti Web Anonimi con OnionShare

La versione 2.2 ha introdotto una funzione inaspettata: l'hosting di pagine web temporanee sulla rete Tor. Immagina di voler condividere una pagina HTML con grafici interattivi, mappe o dashboard, ma senza registrare un dominio o usare servizi di hosting tracciabili.

Come Funziona

Vai alla scheda "Pubblica sito web". Trascina tutti i file necessari (HTML, CSS, JavaScript, immagini). Clicca su "Inizia condivisione". OnionShare genera un indirizzo .onion che chiunque può visitare tramite Tor.

Il tuo computer funge da server. Se lo spegni, il sito scompare. Per mantenere l'indirizzo fisso, attiva "Usa indirizzo persistente" nelle impostazioni. Così, anche riavviando OnionShare, il link rimane lo stesso.

Questa modalità è utile per creare:

• Landing page temporanee per campagne di sensibilizzazione
• Archivi di documenti consultabili via browser
• Dashboard di dati sensibili accessibili solo tramite Tor

Configurazioni Avanzate: Ottimizzare la Sicurezza

OnionShare offre opzioni di personalizzazione che rafforzano la protezione o adattano il comportamento alle tue esigenze.

Timer di Auto-Distruzione

Nelle impostazioni, puoi programmare la scadenza del link. Dopo l'orario impostato, OnionShare interrompe la condivisione automaticamente. Utile se temi di dimenticare il programma aperto.

Password di Accesso

Puoi aggiungere una password al link .onion. Il destinatario dovrà inserirla prima di scaricare i file. Questo livello extra protegge in caso il link venga intercettato.

Notifiche Desktop

Attivandole, ricevi un avviso ogni volta che qualcuno scarica i tuoi file o ne carica di nuovi nella modalità ricezione.

Disabilitare l'Auto-Chiusura

Se preferisci controllare manualmente quando terminare la condivisione, disattiva l'opzione "Interrompi condivisione dopo il primo download". Il link resterà valido finché non lo chiudi tu.

OnionShare vs Altre Soluzioni: Confronto Diretto

WeTransfer, Google Drive, Dropbox Questi servizi archiviano i file sui propri server. L'azienda può accedere ai dati, analizzarli, consegnarli alle autorità se richiesto. I metadati (IP, timestamp, destinatario) vengono registrati.

Send di Mozilla (ora dismesso) Era simile a OnionShare ma meno sicuro: non usava Tor e i file passavano comunque attraverso server di Mozilla.

Magic Wormhole Altro tool open source per trasferimento peer-to-peer. Più veloce di OnionShare ma non anonimizza la connessione. L'IP rimane visibile.

Syncthing Sincronizza cartelle tra dispositivi in modo criptato, ma richiede configurazione complessa e non garantisce anonimato senza Tor.

OnionShare è l'unica soluzione che combina semplicità, anonimato totale e assenza di intermediari.

Limitazioni e Rischi da Conoscere

Nessuno strumento è perfetto. OnionShare ha dei limiti tecnici e operativi.

Velocità di Trasferimento La rete Tor è lenta rispetto a una connessione diretta. File molto pesanti (oltre 1 GB) possono richiedere ore per il download. Se la velocità è prioritaria, OnionShare non è la scelta migliore.

Dipendenza dal Computer Acceso Devi mantenere il computer acceso e OnionShare in esecuzione finché il destinatario non completa il download. Sospensione o riavvio interrompono la connessione.

Nessuna Crittografia End-to-End Persistente I file sono criptati durante il transito, ma una volta scaricati non hanno protezione intrinseca. Se il destinatario li salva su un cloud non sicuro, perdi il controllo.

Possibili Blocchi di Tor Alcuni Paesi censurano la rete Tor. In Cina, Iran o Russia, il destinatario potrebbe non riuscire a connettersi senza VPN o bridge.

Sicurezza Operativa OnionShare protegge la trasmissione, non l'identità di chi condivide il link. Se invii l'indirizzo .onion tramite email non criptata o chat non sicure, chiunque intercetti il messaggio può accedere ai file.

Casi d'Uso Reali

Giornalismo Investigativo Reporter senza frontiere raccomanda OnionShare per ricevere documenti da whistleblower. Il giornalista crea un link di ricezione, lo pubblica su un sito Tor e le fonti caricano i file in modo anonimo.

Indagini OSINT Analisti che raccolgono prove digitali da forum, dark web o social network usano OnionShare per scambiare screenshot, log e dataset senza esporre la loro identità o quella dei collaboratori.

Trasferimento di Backup Criptati Aziende che gestiscono dati sensibili (studi legali, cliniche mediche) usano OnionShare per inviare backup criptati a sedi remote senza affidarsi a Dropbox o servizi simili.

Attivismo Digitale Organizzazioni che operano in regimi autoritari distribuiscono materiale informativo tramite siti Tor hostati con OnionShare, evitando sequestri di server o censure.

Domande Frequenti su OnionShare

OnionShare è legale? Sì, in quasi tutti i Paesi. È uno strumento di sicurezza informatica, come una

VPN o un software di crittografia. L'uso diventa illegale solo se trasferisci materiale vietato dalla legge.

Posso usare OnionShare senza installare Tor Browser? No. OnionShare richiede la rete Tor per funzionare. Se il destinatario non ha Tor, non può accedere ai file.

I file vengono caricati su Internet? No. Rimangono sul tuo computer. OnionShare crea solo un tunnel criptato che permette al destinatario di scaricarli direttamente.

OnionShare funziona su smartphone? Non ufficialmente. Esistono versioni sperimentali per Android, ma sono instabili. La versione desktop resta la più affidabile.

Quanto è difficile intercettare un trasferimento su OnionShare? Teoricamente possibile ma estremamente complesso. Servirebbe controllare tutti i nodi Tor coinvolti nel percorso, cosa che nemmeno le agenzie di intelligence riescono a fare sistematicamente.

Primi Passi con OnionShare: Riepilogo Operativo

Scarica OnionShare da onionshare.org e installa Tor Browser da torproject.org. Avvia OnionShare e attendi la connessione a Tor (10-30 secondi). Per inviare file: vai su "Condividi file", carica i documenti, clicca "Inizia condivisione", copia il link .onion e invialo al destinatario tramite un canale sicuro. Per ricevere file: vai su "Ricevi file", clicca "Avvia modalità ricezione", condividi il link generato con chi deve inviarti i dati.

Le impostazioni avanzate (password, timer, modalità pubblico) si trovano nell'icona ingranaggio in alto a destra. Consulta la documentazione ufficiale su docs.onionshare.org per approfondire.

Vuoi padroneggiare le tecniche OSINT e cybersecurity?

Iscriviti alla newsletter di Coondivido per ricevere guide pratiche, analisi di strumenti e aggiornamenti sulle migliori tecniche di investigazione digitale:

□□ Newsletter: https://coondivido.substack.com/
□□ Telegram: https://t.me/osintaipertutti
□□ Gruppo Telegram: https://t.me/osintprojectgroup
Un'indagine OSINT richiede discrezione. Un caso di cybersecurity ancora di più. Quando invii documenti riservati tramite WeTransfer o Google Drive, lasci tracce digitali: il tuo IP, quello del destinatario, metadati della transazione. Ogni passaggio viene registrato. La domanda è semplice: ti fidi davvero di questi servizi quando gestisci materiale sensibile?

OnionShare risolve questo problema. Si tratta di uno strumento open source del Tor Project che cripta e anonimizza il trasferimento di file, senza intermediari e senza lasciare briciole digitali. I dati partono direttamente dal tuo computer, attraversano la rete Tor e arrivano al destinatario senza passare da server esterni.

Cos'è OnionShare e Come Funziona

OnionShare trasforma il tuo computer in un server web temporaneo accessibile solo attraverso la rete Tor. Quando carichi un file, il programma genera un indirizzo .onion univoco: una stringa alfanumerica che funge da chiave d'accesso. Solo chi possiede questo link può scaricare i dati.

Il meccanismo è diretto. I file non vengono caricati su cloud o piattaforme terze. Rimangono sul tuo disco rigido. OnionShare crea un tunnel criptato che collega il tuo dispositivo a quello del destinatario, passando attraverso i nodi della rete Tor. Ogni connessione viene instradata attraverso tre livelli di crittografia (da qui il nome "onion", cipolla), rendendo impossibile risalire alla sorgente.

Perché la Rete Tor Garantisce l'Anonimato

Tor maschera la tua identità frammentando la connessione attraverso relay sparsi nel mondo.

Nessun nodo conosce l'intero percorso: il primo sa chi sei ma non dove vai, l'ultimo sa dove vai ma non chi sei. Nel mezzo, tutto è criptato.

Questo rende OnionShare ideale per giornalisti che ricevono documenti riservati, ricercatori OSINT che scambiano prove digitali, o professionisti della sicurezza informatica che devono trasferire log di sistema senza esporsi.

Come Installare OnionShare: Procedura Passo-Passo

La configurazione richiede pochi minuti. Prima serve il browser Tor, scaricabile da torproject.org. Senza questo, il destinatario non potrà accedere ai file.

Fase 1: Download e Installazione

Vai su onionshare.org e seleziona il tuo sistema operativo. Il software supporta Windows, macOS e diverse distribuzioni Linux (Ubuntu, Fedora, Debian). Il file pesa circa 50 MB. Dopo il download, esegui l'installer. Su Windows, clicca due volte sul file .exe e segui le istruzioni. Su Linux, apri il terminale e digita i comandi indicati sul sito ufficiale.

Fase 2: Primo Avvio e Connessione a Tor

Apri OnionShare. Una barra di caricamento mostra la connessione alla rete Tor. Il processo dura 10-30 secondi, a seconda della velocità della tua connessione. Quando appare l'interfaccia principale, sei pronto.

L'interfaccia ha tre schede: "Condividi file", "Ricevi file", "Pubblica sito web". Ogni modalità ha uno scopo specifico.

Inviare File con OnionShare: Guida Pratica

Supponiamo di dover inviare un report di analisi forense digitale a un collega. Il documento contiene screenshot di attività sospette e non può transitare su canali non sicuri.

Step 1: Seleziona i File

Vai alla scheda "Condividi file". Trascina il documento nell'area centrale oppure clicca su "Aggiungi" e selezionalo manualmente. OnionShare accetta qualsiasi formato: PDF, immagini, video, archivi compressi. Non ci sono limiti di dimensione, ma file molto grandi richiedono più tempo per il download.

Step 2: Avvia il Server

Clicca su "Inizia condivisione". OnionShare genera un indirizzo .onion, una stringa simile a questa:

http://4acth47i6kxnvkewtm6q7ib2s3ufpo5sqbsnzjpbi7utijcltosqemad.onion/

Questo link è temporaneo e unico. Copialo e invialo al destinatario attraverso un canale criptato (Signal, ProtonMail, Session).

Step 3: Il Destinatario Scarica i Dati

Chi riceve il link deve aprirlo nel browser Tor. Apparirà una pagina minimalista con il pulsante "Scarica file". Cliccando, parte il download. Al termine, OnionShare chiude automaticamente la connessione e cancella il link. Nessuno potrà più accedere a quei dati.

Modalità Pubblico: Condividere con Più Persone

Di default, OnionShare distrugge il link dopo il primo download. Se devi inviare lo stesso file a più destinatari, attiva la "Modalità pubblico" nelle impostazioni (icona ingranaggio in alto a destra). Il link

rimarrà valido finché non interrompi manualmente la condivisione.

Attenzione: questa opzione riduce la sicurezza. Chiunque intercetti il link può accedere ai file. Usala solo quando necessario.

Ricevere File in Modo Anonimo

Rovesciamo lo scenario. Stai conducendo un'indagine OSINT e una fonte vuole inviarti documenti riservati, ma non ha OnionShare installato. Nessun problema.

Step 1: Attiva la Modalità Ricezione

Clicca sulla scheda "Ricevi file". Premi "Avvia modalità ricezione". OnionShare genera un nuovo indirizzo .onion.

Step 2: Condividi il Link

Invia questo indirizzo alla tua fonte. Non serve che installi nulla: basta il browser Tor.

Step 3: Caricamento Remoto

La fonte apre il link nel browser Tor, seleziona i file dal proprio computer e clicca su "Invia file". I dati vengono caricati direttamente sul tuo dispositivo, criptati durante il transito.

OnionShare mostra una notifica quando ricevi nuovi file. Puoi visualizzare la lista cliccando sulla freccia in alto a destra.

Pubblicare Siti Web Anonimi con OnionShare

La versione 2.2 ha introdotto una funzione inaspettata: l'hosting di pagine web temporanee sulla rete Tor. Immagina di voler condividere una pagina HTML con grafici interattivi, mappe o dashboard, ma senza registrare un dominio o usare servizi di hosting tracciabili.

Come Funziona

Vai alla scheda "Pubblica sito web". Trascina tutti i file necessari (HTML, CSS, JavaScript, immagini). Clicca su "Inizia condivisione". OnionShare genera un indirizzo .onion che chiunque può visitare tramite Tor.

Il tuo computer funge da server. Se lo spegni, il sito scompare. Per mantenere l'indirizzo fisso, attiva "Usa indirizzo persistente" nelle impostazioni. Così, anche riavviando OnionShare, il link rimane lo stesso.

Questa modalità è utile per creare:

• Landing page temporanee per campagne di sensibilizzazione
• Archivi di documenti consultabili via browser
• Dashboard di dati sensibili accessibili solo tramite Tor

Configurazioni Avanzate: Ottimizzare la Sicurezza

OnionShare offre opzioni di personalizzazione che rafforzano la protezione o adattano il comportamento alle tue esigenze.

Timer di Auto-Distruzione

Nelle impostazioni, puoi programmare la scadenza del link. Dopo l'orario impostato, OnionShare

interrompe la condivisione automaticamente. Utile se temi di dimenticare il programma aperto.

Password di Accesso

Puoi aggiungere una password al link .onion. Il destinatario dovrà inserirla prima di scaricare i file. Questo livello extra protegge in caso il link venga intercettato.

Notifiche Desktop

Attivandole, ricevi un avviso ogni volta che qualcuno scarica i tuoi file o ne carica di nuovi nella modalità ricezione.

Disabilitare l'Auto-Chiusura

Se preferisci controllare manualmente quando terminare la condivisione, disattiva l'opzione "Interrompi condivisione dopo il primo download". Il link resterà valido finché non lo chiudi tu.

OnionShare vs Altre Soluzioni: Confronto Diretto

WeTransfer, Google Drive, Dropbox Questi servizi archiviano i file sui propri server. L'azienda può accedere ai dati, analizzarli, consegnarli alle autorità se richiesto. I metadati (IP, timestamp, destinatario) vengono registrati.

Send di Mozilla (ora dismesso) Era simile a OnionShare ma meno sicuro: non usava Tor e i file passavano comunque attraverso server di Mozilla.

Magic Wormhole Altro tool open source per trasferimento peer-to-peer. Più veloce di OnionShare ma non anonimizza la connessione. L'IP rimane visibile.

Syncthing Sincronizza cartelle tra dispositivi in modo criptato, ma richiede configurazione complessa e non garantisce anonimato senza Tor.

OnionShare è l'unica soluzione che combina semplicità, anonimato totale e assenza di intermediari.

Limitazioni e Rischi da Conoscere

Nessuno strumento è perfetto. OnionShare ha dei limiti tecnici e operativi.

Velocità di Trasferimento La rete Tor è lenta rispetto a una connessione diretta. File molto pesanti (oltre 1 GB) possono richiedere ore per il download. Se la velocità è prioritaria, OnionShare non è la scelta migliore.

Dipendenza dal Computer Acceso Devi mantenere il computer acceso e OnionShare in esecuzione finché il destinatario non completa il download. Sospensione o riavvio interrompono la connessione.

Nessuna Crittografia End-to-End Persistente I file sono criptati durante il transito, ma una volta scaricati non hanno protezione intrinseca. Se il destinatario li salva su un cloud non sicuro, perdi il controllo.

Possibili Blocchi di Tor Alcuni Paesi censurano la rete Tor. In Cina, Iran o Russia, il destinatario potrebbe non riuscire a connettersi senza VPN o bridge.

Sicurezza Operativa OnionShare protegge la trasmissione, non l'identità di chi condivide il link. Se invii l'indirizzo .onion tramite email non criptata o chat non sicure, chiunque intercetti il messaggio può accedere ai file.

Casi d'Uso Reali

Giornalismo Investigativo Reporter senza frontiere raccomanda OnionShare per ricevere documenti da whistleblower. Il giornalista crea un link di ricezione, lo pubblica su un sito Tor e le fonti caricano i file in modo anonimo.

Indagini OSINT Analisti che raccolgono prove digitali da forum, dark web o social network usano OnionShare per scambiare screenshot, log e dataset senza esporre la loro identità o quella dei collaboratori.

Trasferimento di Backup Criptati Aziende che gestiscono dati sensibili (studi legali, cliniche mediche) usano OnionShare per inviare backup criptati a sedi remote senza affidarsi a Dropbox o servizi simili.

Attivismo Digitale Organizzazioni che operano in regimi autoritari distribuiscono materiale informativo tramite siti Tor hostati con OnionShare, evitando sequestri di server o censure.

Domande Frequenti su OnionShare

OnionShare è legale? Sì, in quasi tutti i Paesi. È uno strumento di sicurezza informatica, come una VPN o un software di crittografia. L'uso diventa illegale solo se trasferisci materiale vietato dalla legge.

Posso usare OnionShare senza installare Tor Browser? No. OnionShare richiede la rete Tor per funzionare. Se il destinatario non ha Tor, non può accedere ai file.

I file vengono caricati su Internet? No. Rimangono sul tuo computer. OnionShare crea solo un tunnel criptato che permette al destinatario di scaricarli direttamente.

OnionShare funziona su smartphone? Non ufficialmente. Esistono versioni sperimentali per Android, ma sono instabili. La versione desktop resta la più affidabile.

Quanto è difficile intercettare un trasferimento su OnionShare? Teoricamente possibile ma estremamente complesso. Servirebbe controllare tutti i nodi Tor coinvolti nel percorso, cosa che nemmeno le agenzie di intelligence riescono a fare sistematicamente.

Primi Passi con OnionShare: Riepilogo Operativo

Scarica OnionShare da onionshare.org e installa Tor Browser da torproject.org. Avvia OnionShare e attendi la connessione a Tor (10-30 secondi). Per inviare file: vai su "Condividi file", carica i documenti, clicca "Inizia condivisione", copia il link .onion e invialo al destinatario tramite un canale sicuro. Per ricevere file: vai su "Ricevi file", clicca "Avvia modalità ricezione", condividi il link generato con chi deve inviarti i dati.

Le impostazioni avanzate (password, timer, modalità pubblico) si trovano nell'icona ingranaggio in alto a destra. Consulta la documentazione ufficiale su docs.onionshare.org per approfondire.

Vuoi padroneggiare le tecniche OSINT e cybersecurity?

Iscriviti alla newsletter di Coondivido per ricevere guide pratiche, analisi di strumenti e aggiornamenti sulle migliori tecniche di investigazione digitale:

□□ Newsletter: https://coondivido.substack.com/
□□ Telegram: https://t.me/osintaipertutti
□□ Gruppo Telegram: https://t.me/osintprojectgroup