



# TOR / Dark Web e principi Crittografici

Fondamenti di Cybersecurity 2022/2023

Davide Berardi <davide.berardi@unibo.it>

La parte di sicurezza informatica che studieremo oggi ha le sue fondamenta in due principi fondamentali: AAA e CIA.

- ▶ Authentication (autenticazione)
- ▶ Authorization (autorizzazione)
- ▶ Accounting (accreditamento)

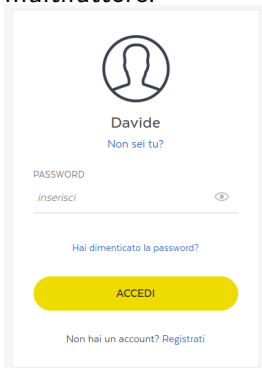
Sono facili da ricordare in questo ordine, senza avere una “proprietà” è difficile garantirne una successiva.

La proprietà di autenticazione è la capacità di un sistema di garantire che un utente possa essere identificato tramite informazioni in suo possesso.

Queste identificazioni possono essere di tre tipi:

- ▶ Quello che si ha (e.g. badge)
- ▶ Quello che si sa (e.g. password)
- ▶ Quello che si è (e.g. impronta digitale)

Se queste informazioni si combinano viene messa in atto la cosiddetta autenticazione multifattore:



A login interface for PostePay. At the top is a circular profile icon. Below it, the name "Davide" is displayed, followed by the link "Non sei tu?". A "PASSWORD" field contains the placeholder text "inserisci" and a toggle icon. Below the password field is a link "Hai dimenticato la password?". A large yellow button labeled "ACCEDI" is centered. At the bottom, a link reads "Non hai un account? Registrati".

Usa il CODICE [redacted] per accedere a PostePay online - Internet Ban... Per migliorare la tua esperienza scarica l'APP!

più meccanismi dello stesso tipo non aumentano la sicurezza!

L'autorizzazione indica che cosa può effettuare un determinato utente.

Esempio: Nel sistema X la password dell'utente può essere cambiata solo da l'utente stesso a fronte di un'autenticazione o un utente speciale (amministratore).

L'accounting è la procedura con cui si assegnano determinate operazioni effettuate a un account (logging).

Ad esempio il traffico consumato dalla propria scheda SIM, quali siti visitate o l'ultima volta che avete cambiato la password.

**Old password**

**New password**

**Confirm new  
password**

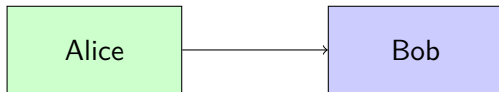
**Change password**

Esistono inoltre altri tre concetti (due saranno **fondamentali** durante il modulo di crittografia).

- ▶ Confidenzialità
- ▶ Integrità
- ▶ Disponibilità

Questi concetti sono indipendenti l'uno dall'altro, la sicurezza di un sistema si può misurare in base a questi tre fattori (che devono essere sempre presenti).

Un messaggio si definisce confidenziale se può essere letto solo dal destinatario predesignato.



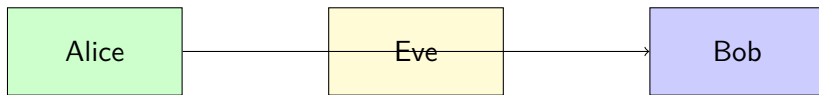
Alice vuole mandare un messaggio a Bob (immaginiamo su whatsapp, mail, teams o telegram), questo messaggio può essere letto solo da Bob.



Ricordiamoci che bisogna pensare come se fosse sempre possibile mettersi nel mezzo di una comunicazione, anche spacciandosi per il destinatario con il mittente e per il mittente con il destinatario.

Questi attacchi prendono il nome di **Man in the Middle**.





Eve, un attaccante nel mezzo cerca di leggere il messaggio per Bob.

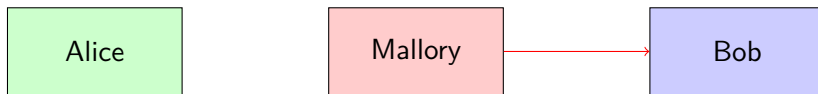
Un messaggio si definisce integro se il destinatario è certo del suo mittente.



Alice vuole mandare un messaggio a Bob (immaginiamo su whatsapp, mail, teams o telegram), Bob è sicuro che arrivi da Alice.



Mallory, un attaccante, modifica un messaggio di Alice inviandolo a Bob (e.g. cambia l'IBAN presente su una fattura).

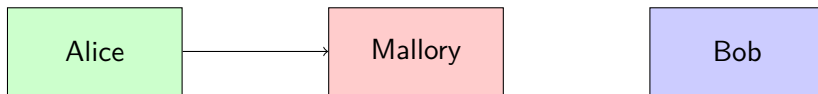


Mallory, un attaccante, si spaccia per Alice e invia un messaggio a Bob.

La disponibilità è la capacità di un sistema di rispondere a determinate richieste.



Alice vuole mandare un messaggio a Bob (immaginiamo su whatsapp, mail, teams o telegram), è garantito che il messaggio arrivi entro un certo tempo.



Mallory, un attaccante nel mezzo, elimina il messaggio per Bob.

Un altro esempio di Denial of Service è un attacco effettuabile per la prenotazione di un ristorante.

1. L'attaccante chiama il ristorante prenotando tutti i coperti



Un altro esempio di Denial of Service è un attacco effettuabile per la prenotazione di un ristorante.

1. Il ristorante non si fida di qualcuno che prenota l'intero ristorante
2. L'attaccante chiama il ristorante  $n/2$  volte prenotando ogni volta un tavolo per 2 persone, dando sempre un nome diverso (spoofing).

Un altro esempio di Denial of Service è un attacco effettuabile per la prenotazione di un ristorante.

1. Il ristorante non si fida di qualcuno che prenota l'intero ristorante
2. Il ristoratore riconosce la voce dell'attaccante e i meccanismi di modifica della voce.
3. L'attaccante e  $n/2$  amici chiamano il ristorante prenotando ogni volta un tavolo per 2 persone. (Distributed denial of service)

Una proprietà non presente in CIA (perché non rappresenta la sicurezza di un sistema ma un modo di eludere la proprietà di accounting) è l'anonimato online.

## Spoiler: Navigando online non siete anonimi.

Siete soggetti a profilazione da parte di ISP (chi vi fornisce la rete), social network, cookies traccianti, etc.

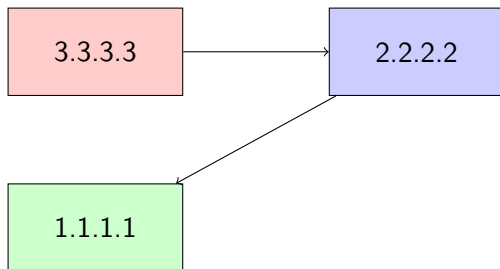
Il protocollo usato a livello globale per identificare un server è Internet Protocol (IP).

La versione 4 prevede indirizzi (che possiamo pensare come numeri di telefono) a 32 bit:

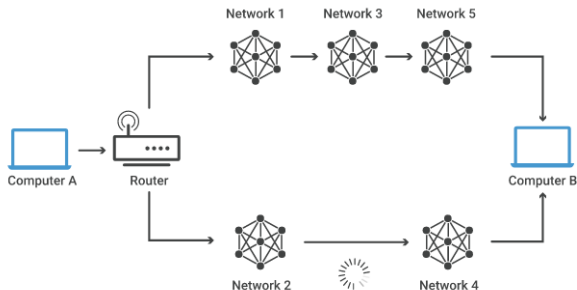


Il server deve conoscere il vostro indirizzo pubblico per rispondere!!! (no anonimato)

Gli indirizzi NON (spoiler: nemmeno i numeri di telefono!) sono protetti da una forma di integrità. Chiunque può cambiare il proprio IP sorgente, esattamente come sulla busta di una lettera.



Non entreremo nei dettagli del routing. Ci limiteremo a dire che, semplicemente, il vostro pacchetto viene fatto passare attraverso un'infrastruttura di router...i quali sono per definizione Man in the Middle!



Al livello superiore, i servizi vengono identificati tramite quella che viene indicata come “porta”. Esempi di porte TCP molto usate sono:

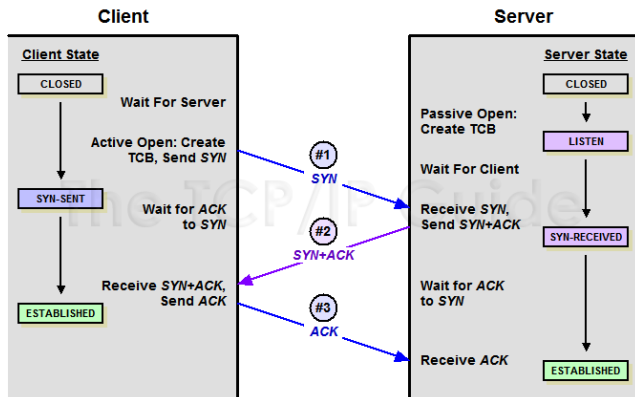
- ▶ 22 SSH
- ▶ 25 SMTP (mail in uscita)
- ▶ 80 HTTP
- ▶ 110 POP (mail in entrata)
- ▶ 443 HTTPS

TCP prevede il concetto di connessione, a differenza di altri protocolli dello stesso livello (UDP).

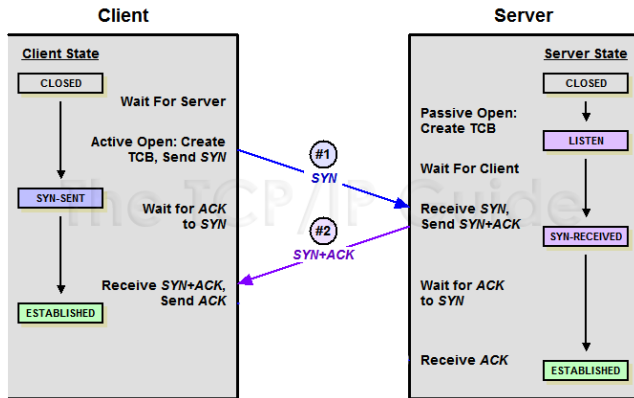
Sempre nel mondo dei telefoni possiamo pensare a questo concetto come una chiamata.

Per effettuare questa operazione TCP invia un pacchetto con una segnalazione speciale chiamata SYN, si aspetta un pacchetto con una segnalazione SYN-ACK e, per “rispondere” correttamente deve inviare un pacchetto contenente una segnalazione ACK.





Cosa succede se non si invia mai l'ACK finale e il server può accettare al massimo n connessioni?



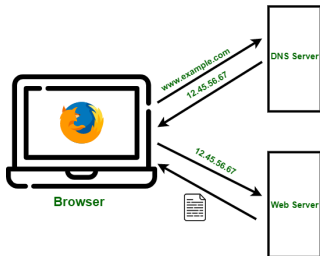
Cosa succede se non si invia mai l'ACK finale e il server può accettare al massimo  $n$  connessioni?

## Denial of Service dopo $n$ “chiamate”!

Ricordiamo l'esempio del ristorante.

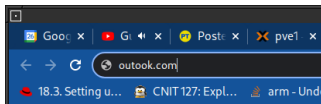
Il mondo dei servizi online non ragiona con indirizzi (sarebbe quasi impossibile non sbagliare un'indirizzo email...pensate se per inviarmi una mail dovreste ricordarvi `davide.berardi@137.204.24.147 ...`).

Per questo motivo esiste un registro online distribuito chiamato DNS.



Cosa succede se compriamo il dominio  
gmail.it?


Tutte le persone che sbaglieranno a scrivere un indirizzo gmail.com invieranno una mail al nostro server. Questo fa in modo di ottenere email private senza nemmeno dover usare social engineering.



Lo sniffing è una forma di Eavesdropping, può essere fatto (e normalmente viene messo in atto) da chiunque lungo il percorso verso la vostra destinazione.

## Security by Obscurity

In tutti i protocolli che abbiamo elencato è possibile fare sniffing (e.g. sniffing DNS rivela a che siti state facendo richiesta, sniffing TCP cosa state chiedendo al server, etc).



The toolbar contains various icons for file operations (open, save, print, etc.), search, and navigation (back, forward, etc.).

icmp				
No.	Time			Source
3	2021-04-26	18:16:47.702410820	130.136.4.127	
4	2021-04-26	18:16:48.675862625	10.0.2.15	
5	2021-04-26	18:16:48.699709363	130.136.4.127	
6	2021-04-26	18:16:49.677022586	10.0.2.15	
7	2021-04-26	18:16:49.700911343	130.136.4.127	
8	2021-04-26	18:16:50.677407350	10.0.2.15	
9	2021-04-26	18:16:50.701587524	130.136.4.127	



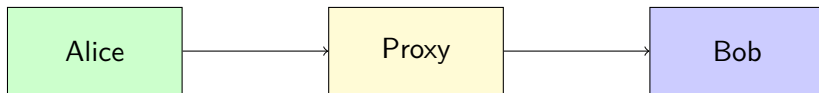
Prendiamo in considerazione un caso più semplice: l'invio di mail anonime.

Un anonymous remailer è un server che ricevuta una mail (con le informazioni sul destinatario) la inoltra al destinatario rimuovendo le informazioni del mittente.

È il concetto alla base di VPN come NordVPN



Un Anonymous Remailer è un esempio di Proxy. Il problema dei proxy è che il proxy ha informazioni su di voi (e può agire da eavesdropper).

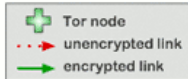


Per anonimizzare completamente il traffico è possibile usare il cosiddetto Routing “a Cipolla” (Onion Routing).

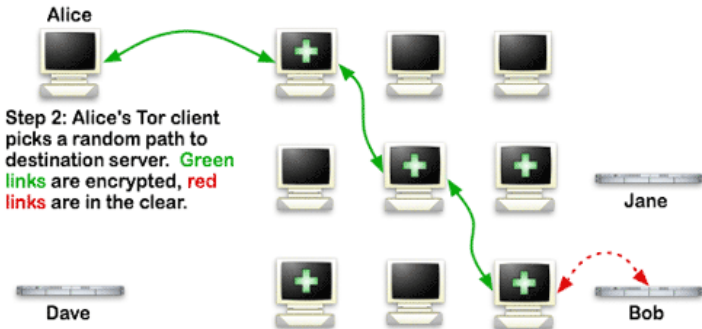
Il software Tor (The Onion Router) utilizza questi concetti per anonimizzare il traffico. Sviluppato come software open source dal 2002.



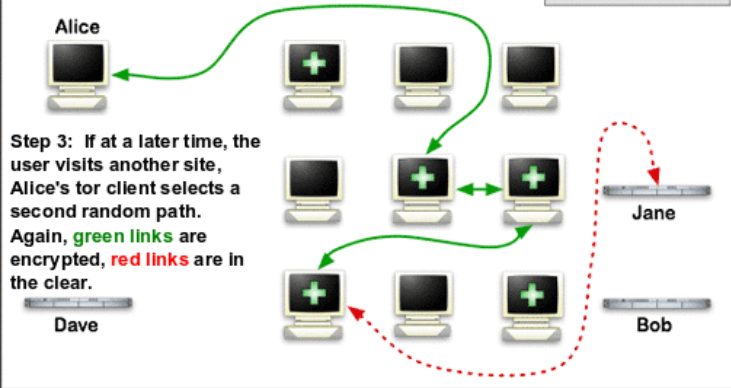
## How Tor Works: 1

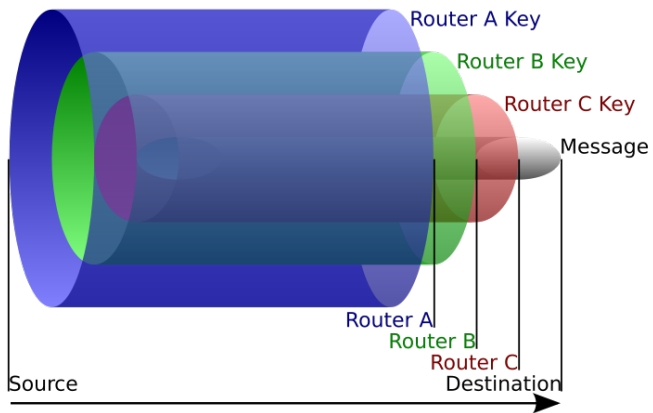


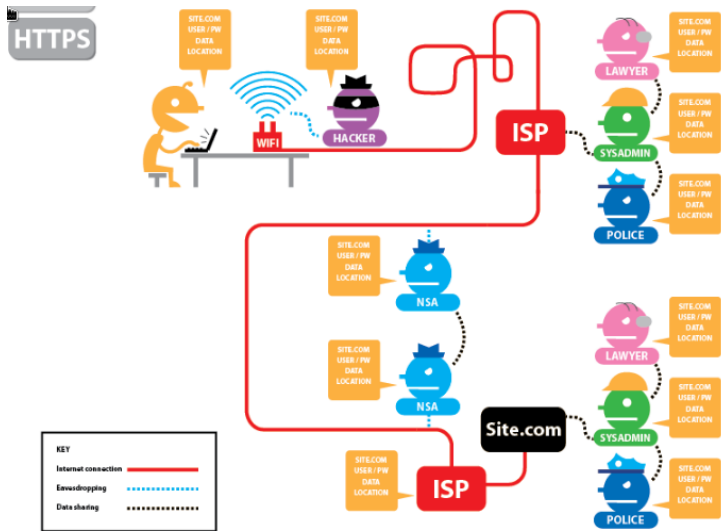
## How Tor Works: 2



## How Tor Works: 3









Tor quindi viene denominata come rete “overlay”. Una rete chiusa al quale interno vengono distribuiti dati in forma anonima. Questo è il principio dei servizi onion.

Esistono alcuni servizi su Tor in grado di farvi uscire sulla rete “normale”. Vengono chiamati Exit Node.

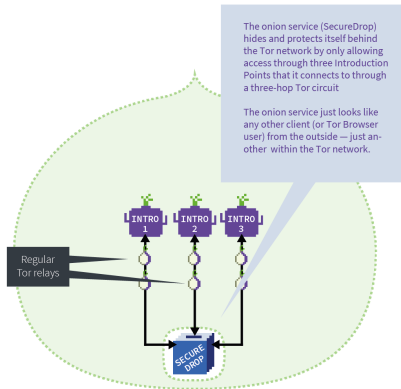
Attenzione: chi mantiene l'exit node vede tutto il vostro traffico!

Attenzione 2: essendo pubblici sono normalmente bloccati da ogni servizio (e.g. banche).

## 🔥 ONION SERVICE

1/9

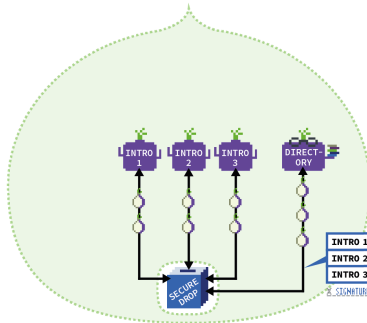
Your local newspaper decides to set up an onion service (using SecureDrop) to receive anonymous tips. All onion services must be set up inside the protection of the Tor network.



### ONION SERVICE

2/9

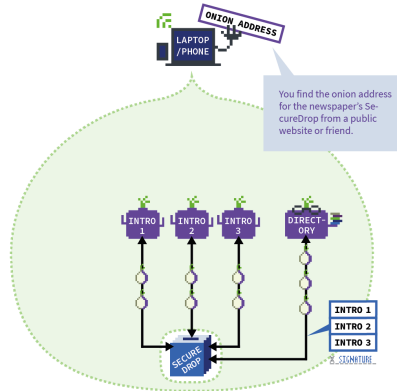
It advertises these Introduction Points on a directory server by creating a descriptor: 3 Introduction Points addresses and a public key, all signed by the service's private key.



### ONION SERVICE

3/9

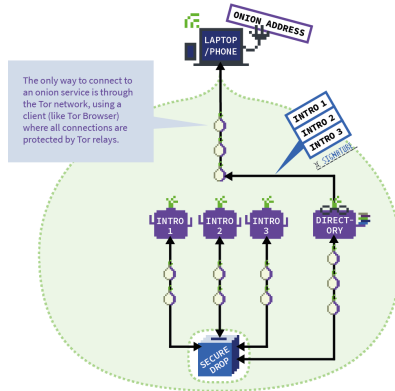
Say, you want to anonymously send some tax fraud data to your local newspaper's through its SecureDrop.



 **ONION SERVICE**

You request more information about the onion address from the directory server.

4/9

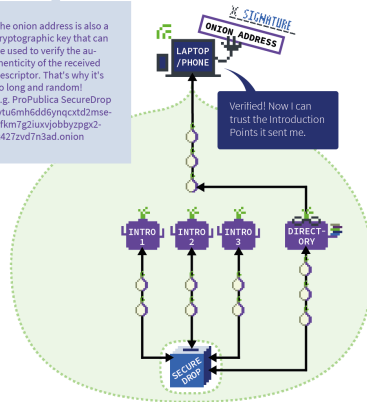


### ONION SERVICE

5/9

You use the key embedded in the onion address and the signature from the service to verify what you've received.

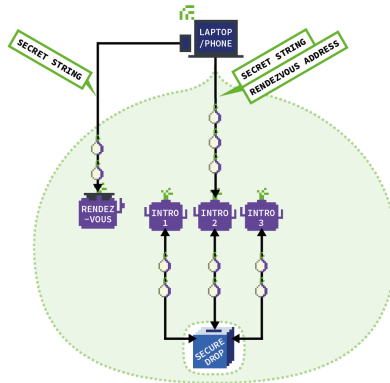
The onion address is also a cryptographic key that can be used to verify the authenticity of the received descriptor. That's why it's so long and random!  
E.g. ProPublica SecureDrop  
lvtu6mh6dd6ynqcxtd2mse-qfkm7g2iuxvjobbyzpgx2-jt427zvd7n3ad.onion



### ONION SERVICE

6/9

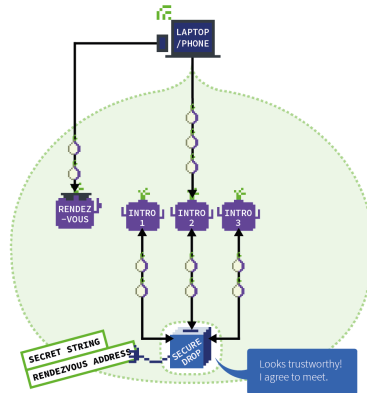
- Then you: 1. Set up a neutral rendezvous point  
2. Ask for an "introduction" to the onion service/  
SecureDrop from one of the Introduction Points.



### ONION SERVICE

7/9

The Introduction Point passes your details on to the onion service, who runs multiple verification processes to decide whether you're trustworthy or not.

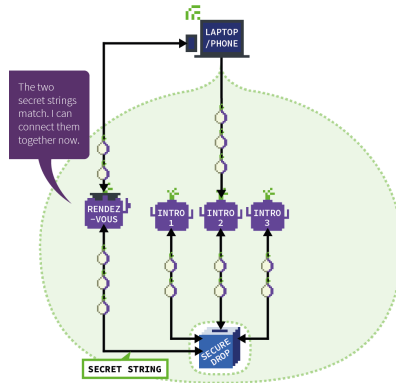




### ONION SERVICE

8/9

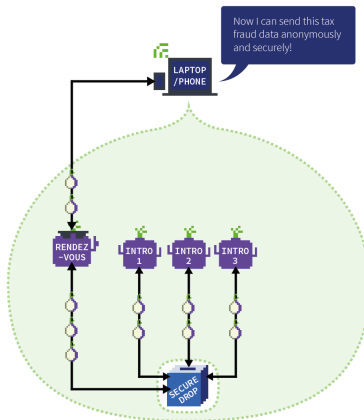
The rendezvous point makes one final verification to match the secret strings from you and service (the latter also comes from you but has been relayed through the service).



## 🔥 ONION SERVICE

9/9

Using the rendezvous point, a Tor circuit is formed between you and your newspaper's SecureDrop onion service.



Grazie all'anonimato offerto dai servizi onion (sia di chi visita che di chi fa hosting). È inevitabile che si siano sviluppati dei servizi illegali al suo interno. Alcuni esempi:

- ▶ Compravendita di materiale illegale (droga, armi);
- ▶ Servizi di hacking;
- ▶ Servizi di assassinio su commissione;
- ▶ Pornografia illegale;
- ▶ ...

Ovviamente l'affidabilità di questi servizi è sempre in dubbio. Quanti di questi possono essere “esche”?

Questo non rende l'uso di Tor illegale, né automaticamente illegale ogni servizio al suo interno (addirittura faremo un'esercitazione su Tor e un servizio onion).

Dovrete invece essere in grado di usarlo e di conoscerlo per proteggervi da eventuali attacchi (torniamo sempre alla Security by Obscurity).

Un comportamento molto presente sui servizi onion, soprattutto grazie alla compravendita illegale, è quello dei Dataleak.

Un dataleak è un rilascio di informazioni private di aziende, persone o oggetti (e.g. codice sorgente).



Un Dataleak di tipo Fullz è una collezione di informazioni personali almeno contenenti il minimo indispensabile per creare conti-correnti e/o pagare con carte di credito.

Alcuni esempi:

- ▶ Nome e Cognome
- ▶ Data di nascita
- ▶ Codice Fiscale
- ▶ Indirizzo di residenza
- ▶ Numero di telefono

Tramite questi leak è possibile perpetrare truffe molto più facilmente (Spoofing).

I leak più comuni rimangono quelli di account e password. In questo caso una lista di account viene messa online, sperabilmente (dal punto di vista dell'attaccante) con password in chiaro (vedremo nel modulo di crittografia come ci si protegge da ciò).

#### NORD VPN Accounts:

m[REDACTED]@gmail.com:c[REDACTED]13

1[REDACTED]02@gmail.com:1[REDACTED]I

[REDACTED]@icloud.com:c[REDACTED]1

[REDACTED]@gmail.com:D[REDACTED]0

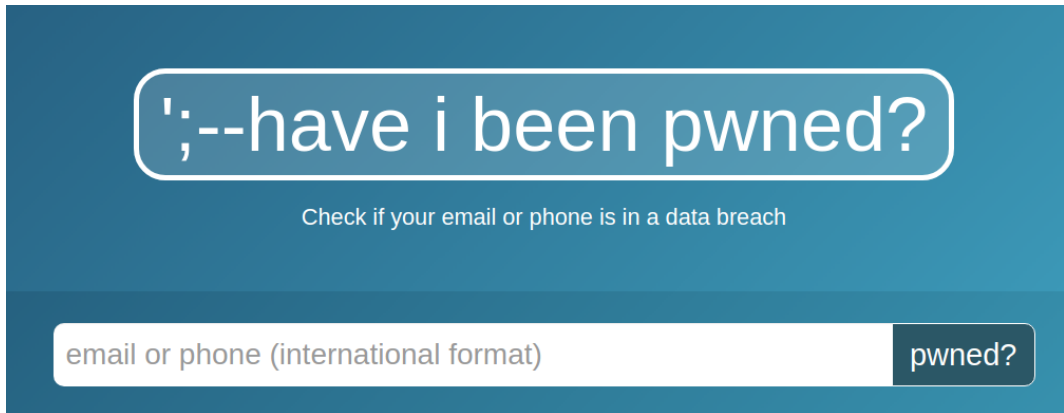
[REDACTED]@gmail.com:r[REDACTED]0

[REDACTED]@yahoo.com:c[REDACTED]13

[REDACTED]@gmail.com:1[REDACTED]2

[REDACTED]@hotmail.com:f[REDACTED]0

Esistono sistemi online in grado di allertarvi quando viene pubblicato un leak contenente il vostro account, il più famoso è haveibeenpwned.



The image shows the homepage of the 'Have I Been Pwned?' website. It features a dark blue background. At the top, there is a light blue rounded rectangle containing the text 'have i been pwned?' in a white, lowercase, sans-serif font. Below this, the text 'Check if your email or phone is in a data breach' is displayed in a smaller, white, sans-serif font. At the bottom, there is a white input field with the placeholder text 'email or phone (international format)' in a grey, sans-serif font. To the right of the input field is a dark blue button with the text 'pwned?' in a white, sans-serif font.

Mentre HavelBeenPwned è gestito da un'organizzazione esterna, è possibile utilizzare alcuni software in grado di scandagliare la rete (crawler / spider) alla ricerca di leak che contengono determinate stringhe. Questi software sono in grado di scandagliare anche i principali mercati neri tramite insider.

#### Browse important pastes

Year: 2018

Credentials Credit cards SQL injections CVEs Keys API Keys Mails Phones Omons Bitcoin Base64

Show 10 entries

Search:

#	Path	Date	# of lines	Action
0	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/19/2vnpBUk2.gz</a>	2018/06/19	37	<a href="#">🔍</a>
8	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/19/ksDaeE3.gz</a>	2018/06/19	244	<a href="#">🔍</a>
1841	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/19/3NasYKD.gz</a>	2018/06/19	3714	<a href="#">🔍</a>
1856	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/18/5uPufFQL.gz</a>	2018/06/18	232	<a href="#">🔍</a>
2	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/17/CXnzQdM.gz</a>	2018/06/17	386	<a href="#">🔍</a>
1826	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/17/7Ue68j.gz</a>	2018/06/17	19	<a href="#">🔍</a>
1838	<a href="#">/home/ailgit/AIL/framework/PASTES/alerts/pastebin.com_gpro2018/06/17/qweYJnC.gz</a>	2018/06/17	529	<a href="#">🔍</a>
1839	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/17/vZqzh8.gz</a>	2018/06/17	56	<a href="#">🔍</a>
1825	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/16/jvth8th.gz</a>	2018/06/16	44	<a href="#">🔍</a>
1837	<a href="#">/home/ailgit/AIL/framework/PASTES/archive/pastebin.com_gpro2018/06/16/f4fX08ei.gz</a>	2018/06/16	110	<a href="#">🔍</a>

Showing 1 to 10 of 50 entries

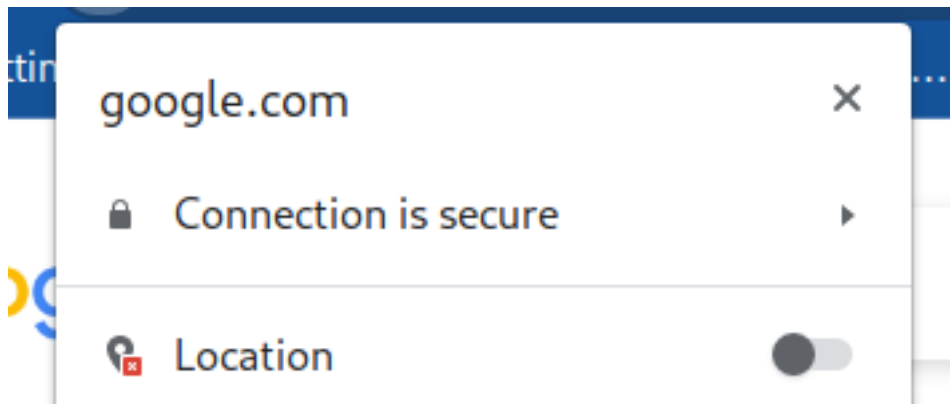
Previous 1 2 3 4 5 Next

Possibile tesi!



Tor non è perfetto. La rete è principalmente contraria all'anonimato. Ad esempio esistono alcune problematiche che possono rivelare l'IP di chi sta accedendo a un determinato servizio.

Primo fra tutti la geolocalizzazione



Anche la richiesta di informazioni al DNS (soggetta a sniffing o anche controllata dal gestore del DNS) è in grado di rivelare cosa state cercando di accedere.

Supponiamo di voler accedere al sito

`silk4lfaq47vh5mzs4p2vhmfuymqg76ylhayylo2isplyef72corepad.onion` (silkroad, mercato nero online) da un account Unibo. Una richiesta DNS per richiedere il sito potrebbe essere inviata fuori da Tor e gli sniffer saprebbero che state cercando di accedere a quel sito!

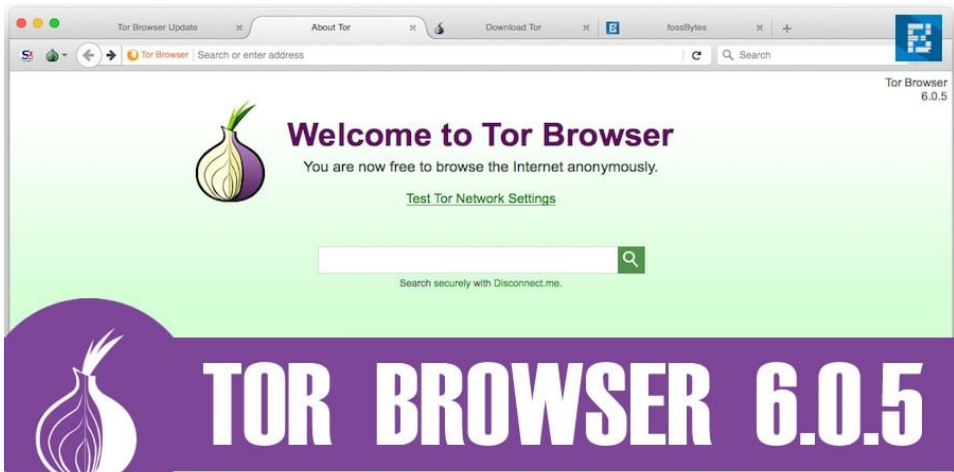
Le informazioni rivelate non devono per forza essere direttamente collegate a vostre richieste ma possono essere informazioni “lateralali” a cui non avete pensato.

Esempio: Se siete soliti mantenere il vostro browser in finestra con una dimensione precisa, queste informazioni potrebbero essere inviate al server remoto (tramite javascript) e questo potrebbe profilarvi con precisione!

Rilasciare più informazioni del necessario o poter utilizzare più strumenti rispetto a quelli strettamente necessari è un problema concettuale di sicurezza.

Dovreste limitare le capacità di un software al minimo indispensabile richiesto (e.g. se siete i proprietari di un albergo perché girare sempre con un passe-partout quando magari dovete aprire nel 90% dei casi una singola porta?)

Per evitare queste problematiche esiste una versione di firefox modificata già configurata per non rilasciare più informazioni del necessario (privilegio minimo).

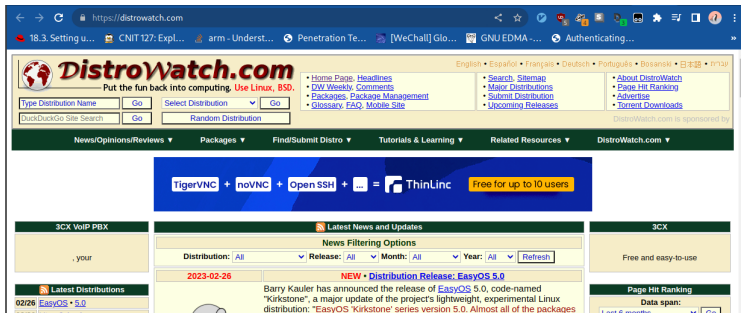


Purtroppo, queste problematiche possono sussistere non solo nel browser ma anche a livello di sistema operativo. Esiste una Distribuzione Linux chiamata Tails, la quale vi predispone il sistema per l'essere il più anonimo possibile.



Una distribuzione Linux (Linux non è un sistema operativo!!!! è un Kernel) è un'insieme di software configurato per un determinato scopo.

Esistono distribuzioni per i server (Debian, Centos, ...), distribuzioni per il desktop (Ubuntu, Manjaro, ...), distribuzioni per la produzione audio (UbuntuStudio, ...), etc, etc.



Domande?