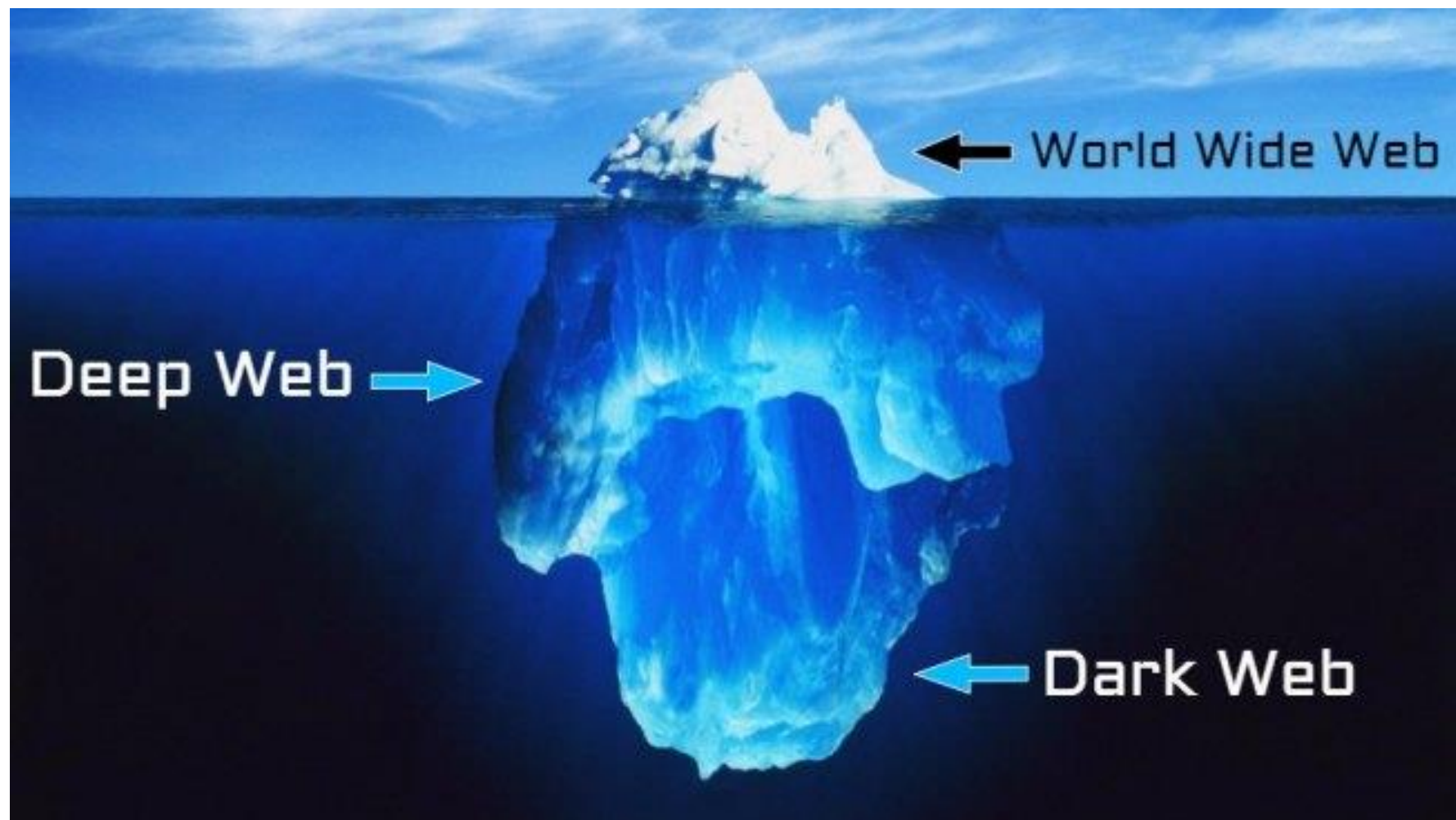


# Deep Web

Il lato oscuro del Web

## Deep Web

*“Dove tutto accade e dove si aggirano  
entità quasi mitologiche”*



← World Wide Web

Deep Web →

← Dark Web

# Deep Web

Con il termine Deep Web si indica l'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (ad es. Google, Bing)

# Dark Web

Con il termine Dark Web si indica l'insieme di contenuti accessibili pubblicamente che sono ospitati in siti web il cui indirizzo IP è nascosto, ma ai quali chiunque può accedere purché ne conosca l'indirizzo

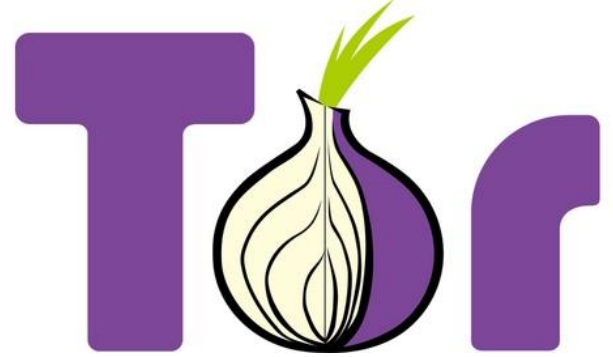
# DarkNet

Elementi appartenenti al Dark Web sono anche i contenuti privati scambiati tra utenti all'interno di un network chiuso di computer, strutture definite come darknet

# Reti Darknet

- TOR (The Onion Router)
- The Invisible Internet
- Project (I2P)
- Freenet
- anoNet

TOR



Consente di anonimizzare l'accesso a internet dei suoi utenti e proprio le condizioni di pseudo-anonimato che essa offre la rendono un elemento di attrattiva per organizzazioni dedite al crimine informatico



# TOR


Difficoltà delle forze dell'ordine a svolgere operazioni di monitoraggio su larga scala e la funzione di aggregatore che si riconosce ai principali black market che la rete ospita



Le dimensioni contano?

# Surface Web


La rete visibile e che ha contenuto che può essere trovato utilizzando motori di ricerca come Google o Yahoo, e soprattutto è sotto costante sorveglianza da parte dei governi, rappresenta il **4%** dei contenuti del world wide web



4%


Surface Web





# 96%

Deep Web



## Surface Web

YAHOO!

Google

reddit

CNN.com

bing

## Deep Web

Academic databases  
Medical records  
Financial records  
Legal documents  
Some scientific reports  
Some government reports  
Subscription only information  
Some organization-specific  
repositories

## Dark Web

TOR  
Political protest  
Drug trafficking  
and other illegal activities

**96%**

of content on the  
Web (estimated)

# Come funziona TOR?

Applicativo che consente di navigare sul web in totale anonimato, basandosi su una versione modificata di Mozilla Firefox che non rilascia informazioni personali in Rete

# Volete provare?

<https://www.torproject.org/download/download-easy.html.en>



# Chi viaggia sul Deep Web?

Un'analisi dei contenuti consente la facile verifica della presenza di gruppi di criminali, hacktivist, script kiddies, giornalisti, dissidenti, terroristi e molto probabilmente agenzie di intelligence

# Cosa troviamo nel Deep Web?

Ricerche scientifiche

Database medici

Forum privati

Documenti finanziari



## E nella Darknet?

Il dark web è un luogo particolarmente interessante per le comunità di sviluppatori di malware e per i loro clienti. Nel molti black market che vi risiedono è molto semplice reperire codici malevoli e servizi utili alla personalizzazione e distribuzione di malware

## I costi?

Per acquistare un malware è possibile spendere da poche decine fino a qualche migliaio di dollari per un servizio di personalizzazione completa di un codice malevolo

# Prezzi

Un record contenente informazioni personali di un utente è venduto a \$1

# Prezzi

Account PayPal ed eBay sono acquistabili  
a partire da \$300

## Prezzi

Account per online banking sono venduti a prezzi compresi tra \$200 e \$500 in funzione del saldo contabile e della relativa storia

## Prezzi

Le scansioni di documenti di identità e patenti sono acquistabili per una cifra compresa tra i \$10 ed i \$35



## Prezzi

Hackerare un account Facebook, Twitter o di altre piattaforme di social networking può costare dai \$50 ai \$200 dollari

## Prezzi

Il codice sorgente di un malware bancario con annessa personalizzazione è offerto per una cifra dai \$900 ai \$1500



\$300,000 ai \$500,000 al  
giorno

Giro d'affari





Esempio del 30 Gennaio  
2019

## xDedic

Gestito da 3 hacker in Ucraina, vendeva o affittava le chiavi di accesso a computer o server sparsi in tutto il mondo e ha facilitato il traffico di informazioni identificative personali di cittadini statunitensi

## xDedic

Offriva ai cybercriminali interessati la possibilità di cercare più di **176 mila server compromessi** ottenendo le credenziali di accesso remoto provenienti da tutto il mondo e ricercabili secondo una catalogazione per prezzo, sistema operativo o persino per posizione geografica di origine del file rubato

## xDedic

Questo mercato underground per hacker ha permesso attacchi cibernetici contro infrastrutture del governo locale statale o federale degli Stati Uniti, reti ospedaliere, servizi di emergenza, studi legali, contabili e fondi pensione..

xDedic

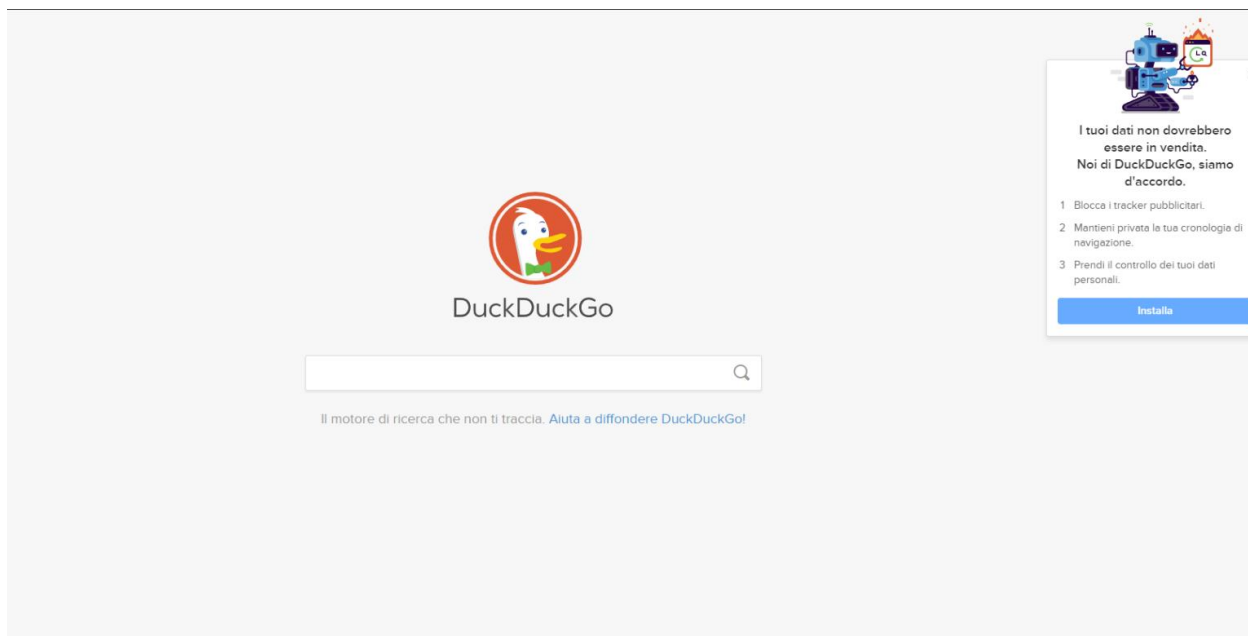
Costo minimo di 6 dollari



xDedic

**Ha guadagnato più di 68  
milioni di dollari**

# Vuoi avere privacy senza entrare nel Deep Web?



# Approfondimento

<https://www.youtube.com/watch?v=Mtq9dkJDfjo>

<https://www.alground.com/site/deep-web-dark-cose/51954/>