UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Darkweb & Cryptominer

Claudio Sardini

Conerobus S.p.a.
c.sardini@conerobus.it

Martedì 19 Luglio 2022

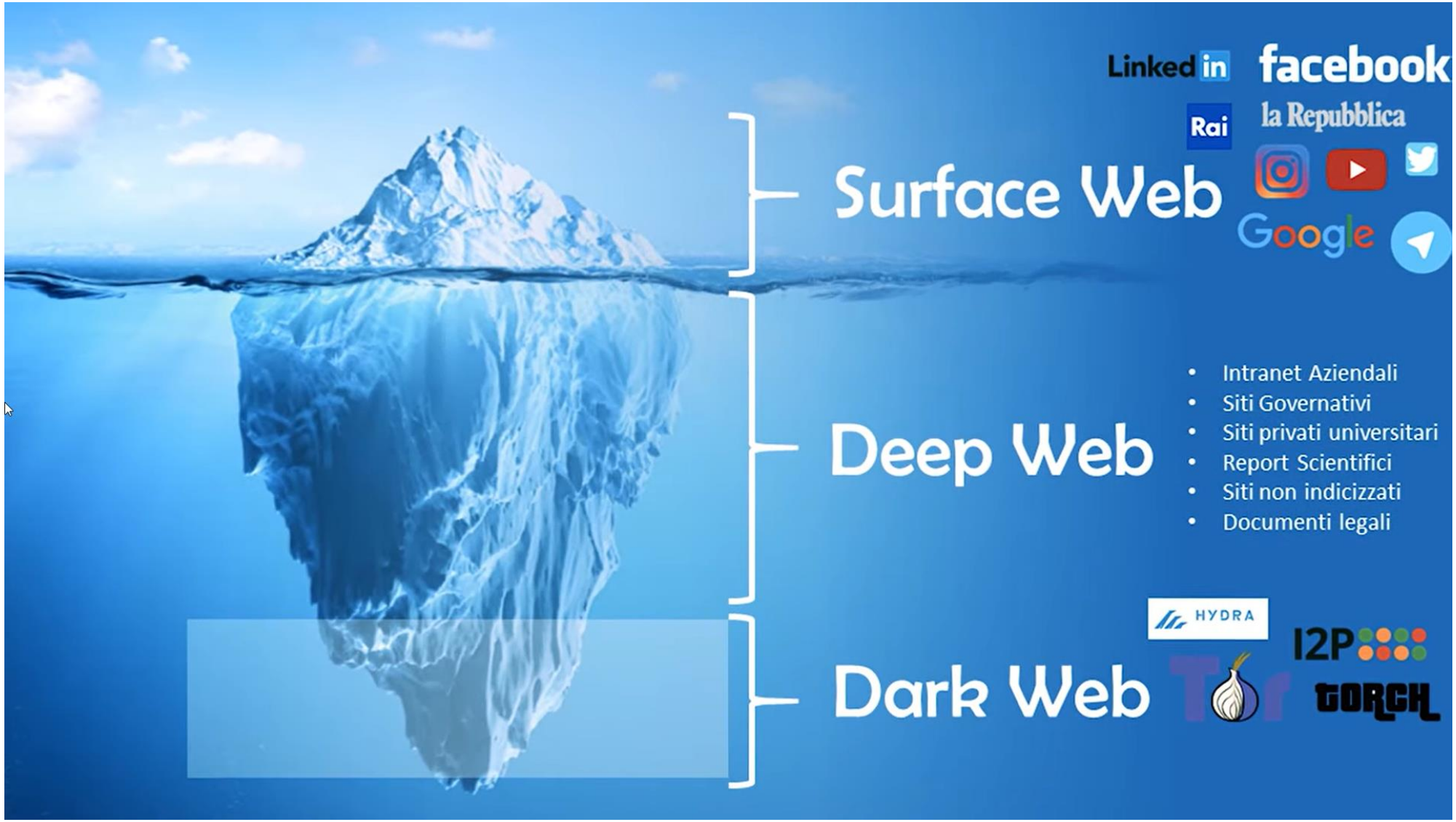
Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

ARGOMENTI

- I tre tipi di web
- Navigazione anonima
- The Onion Router – TOR
- Ricerche
- Da dato a valore
- Ransomware
- Cryptominer

I tre tipi di web

INTERNET...


Linked in
facebook
Rai
la Repubblica
Surface Web
Google
Deep Web
Intranet Aziendali
Siti Governativi
Siti privati universitari
Report Scientifici
Siti non indicizzati
Documenti legali
HYDRA
I2P
Dark Web
Tor
TORCH

SURFACE WEB O CLEAR WEB

- Tutti i contenuti internet direttamente raggiungibili e ricercabili in quanto normalmente indicizzati dai motori di ricerca e/o registrati con nomi ai principali livelli di dominio.
- Si stima che rappresenti circa il 6% dell'interno contenuto

Deep Web

- Tutto ciò che non è direttamente raggiungibile e/o rintracciabile attraverso i normali motori di ricerca.
  - Siti intranet
  - Raccolte di documenti privati
  - Pagine web non registrate nei DNS
  - Ecc…
- Quasi il 90% dei contenuti appartengono al Deep Web

DARK WEB

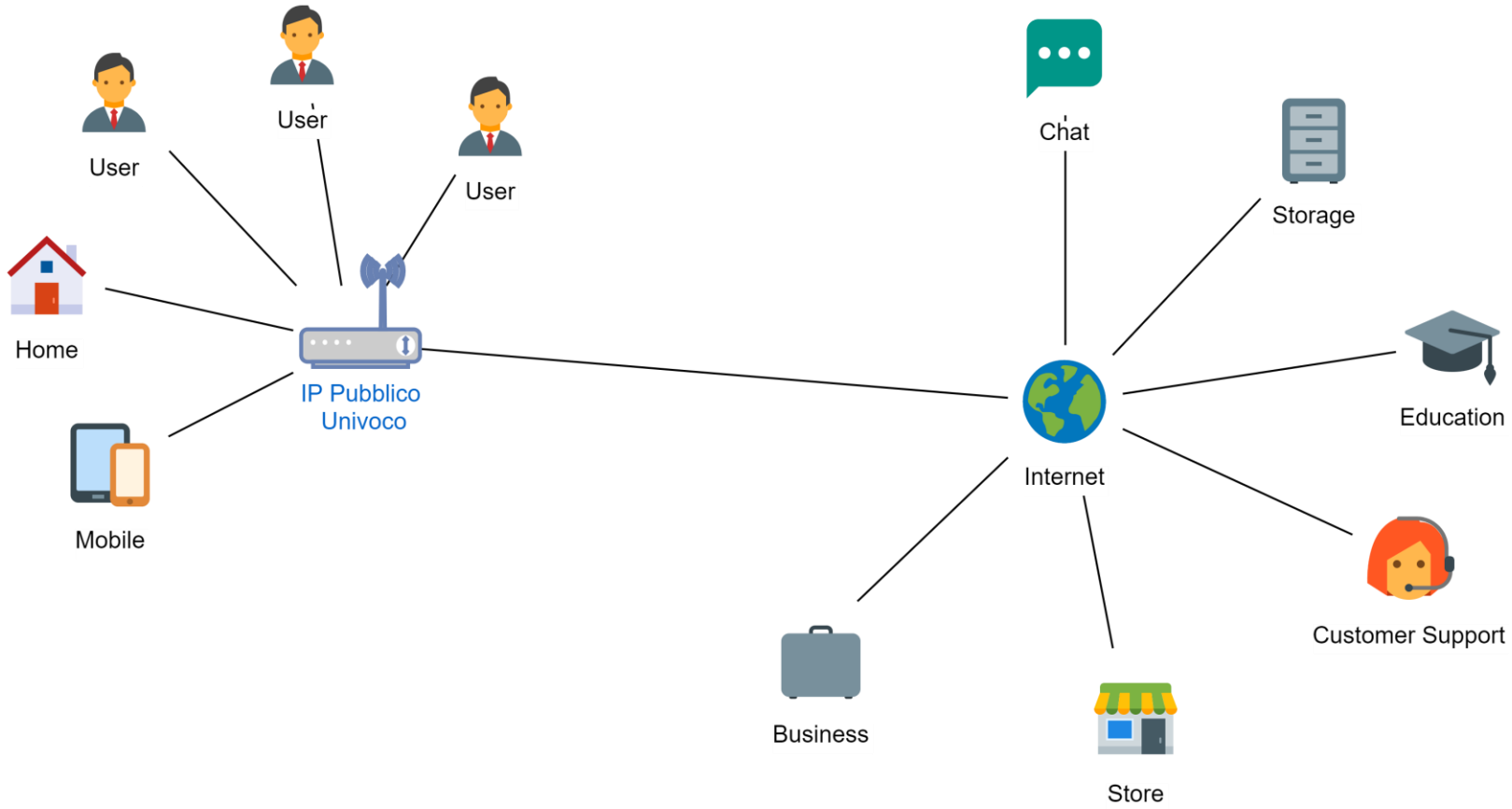
- Siti non raggiungibili attraverso i normali circuiti di ricerca né tramite URL standard
- Servono sistemi di navigazione appropriati per raggiungerli
- Non sono indicizzati(*)
- Nati per libertà di opinione e anonimato, oggi ospitano un po' di tutto

Navigazione anonima

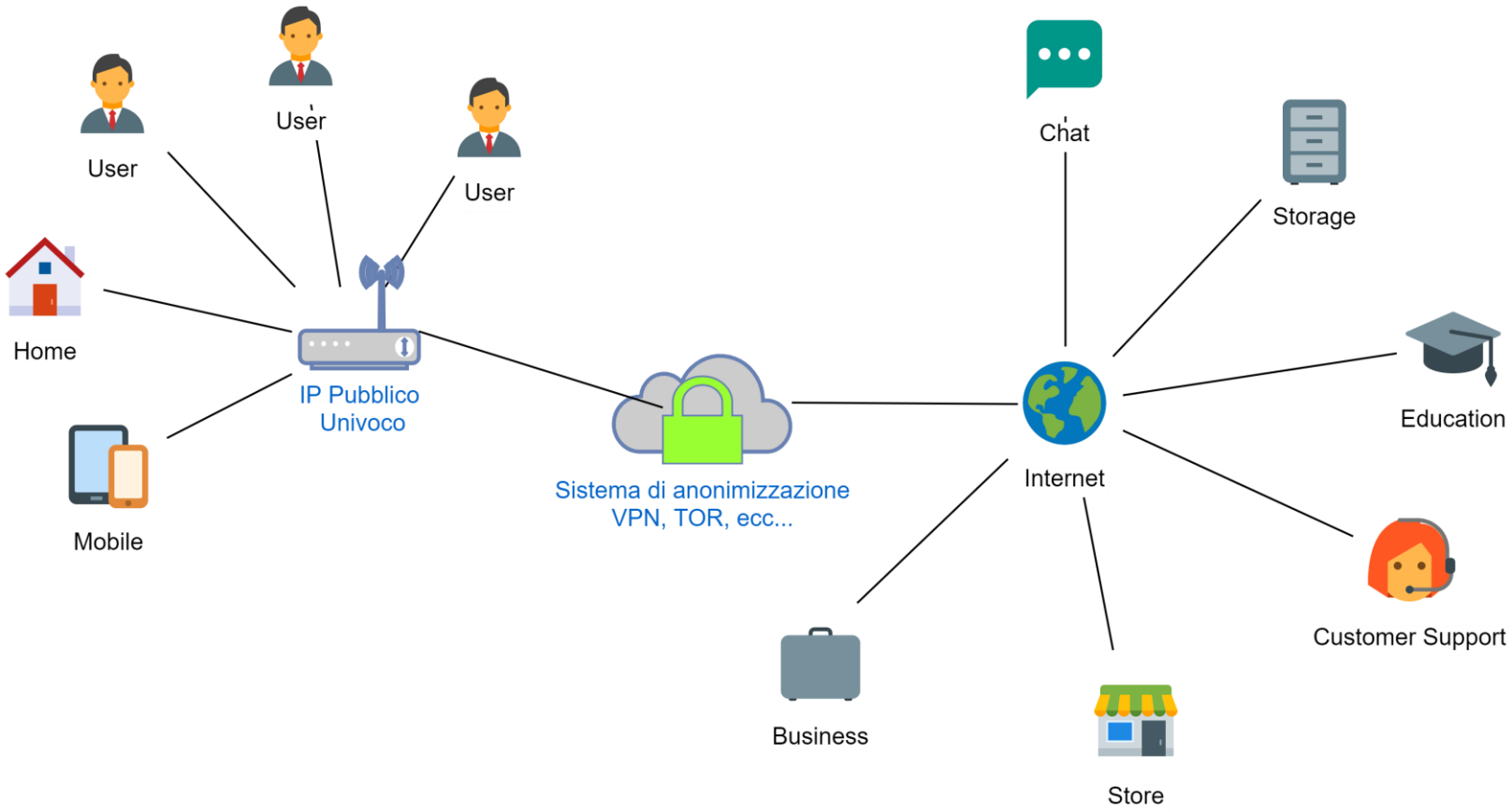
NAVIGAZIONE ANONIMA

- L’opzione di navigazione in incognito è presente ormai in tutti i browser ma in realtà non ci permette di navigare in maniera totalmente anonima.
- Tale opzione non nasconde il nostro indirizzo IP e permette ai siti web che visitiamo di ottenere informazioni riguardo la provenienza della connessione, il SO utilizzato e anche la versione di browser installata.

NAVIGAZIONE ANONIMA



NAVIGAZIONE ANONIMA

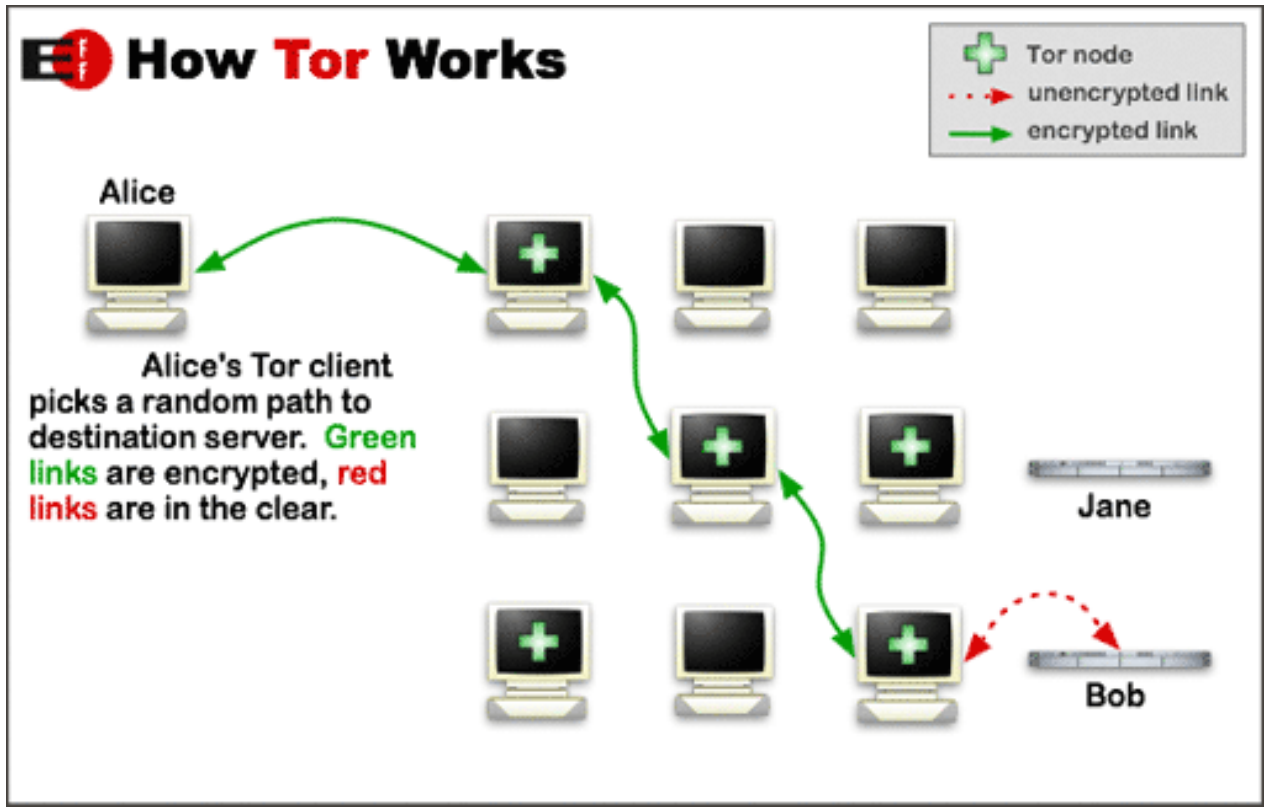


TOR – The Onion Router

TOR

- Per nascondere e cambiare frequentemente il nostro indirizzo IP un browser adatto da utilizzare per la navigazione è **Tor Browser**.
- E' una versione modificata del browser Mozilla che permette di navigare totalmente anonimi poiché in automatico effettua una connessione alla rete TOR (*The Onion Router*).
- In tale rete il traffico dati non viaggia in maniera tradizionale direttamente da client a server e viceversa ma viene veicolato attraverso un circuito virtuale più complesso e cifrato composto da una moltitudine di *Onion Router*.

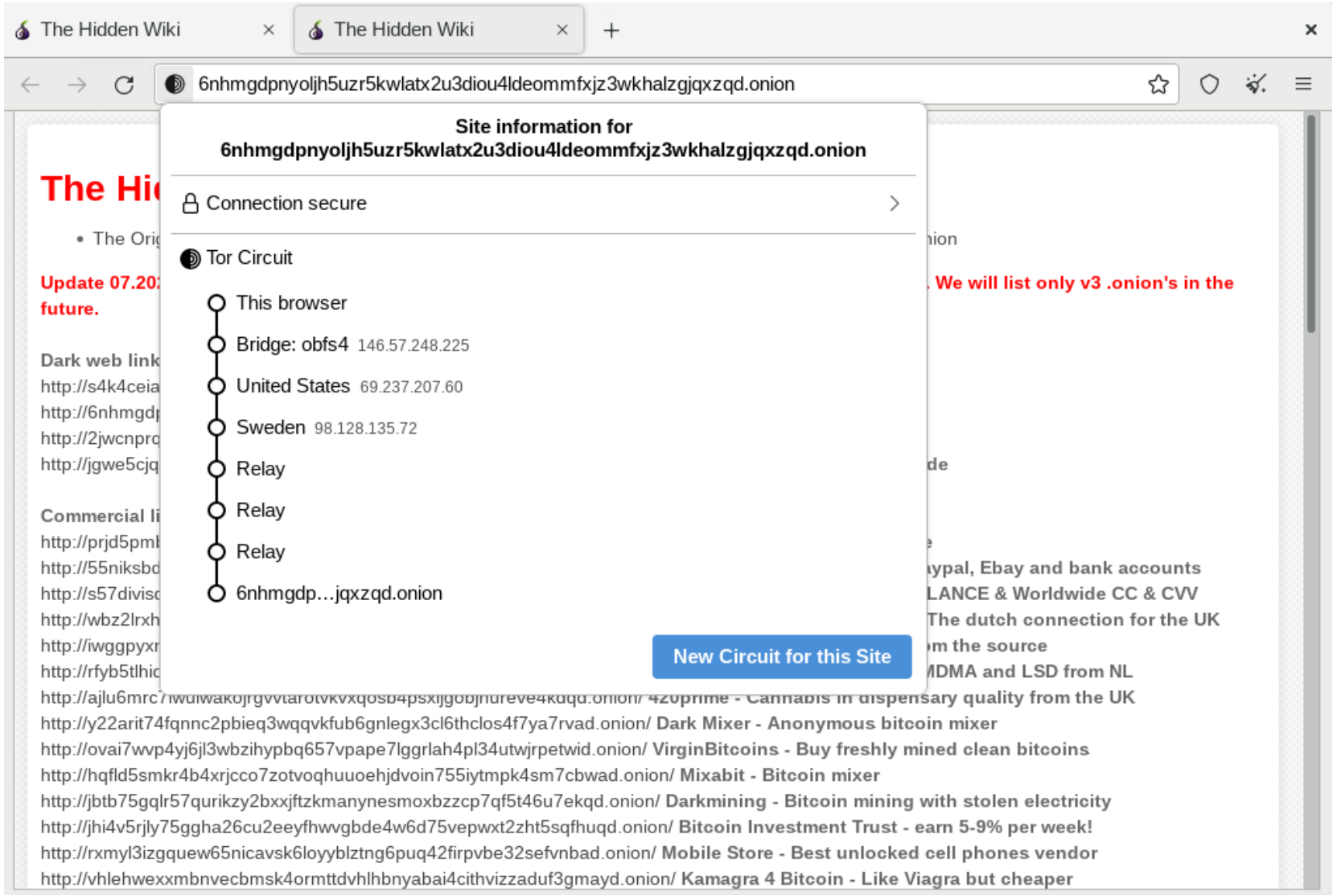
ONION RINGS

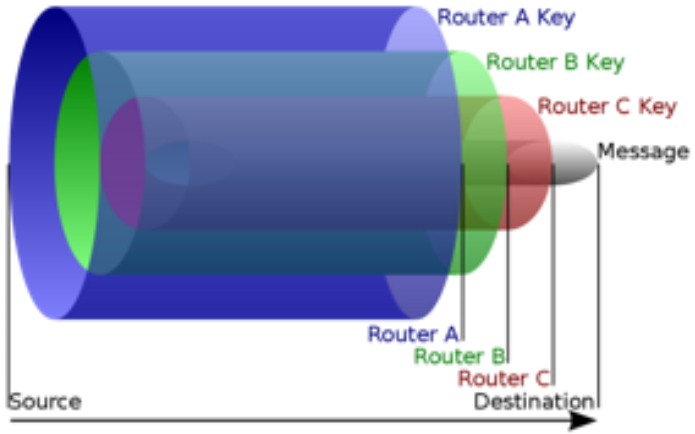

How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

ONION RINGS

- Una volta che l'utente ha composto il messaggio da inviare, il browser TOR, seleziona tre server di TOR in maniera casuale.
- Il software crea un percorso tra questi tre server iniziando con il crittografare il messaggio ed inviarlo al primo server, ovvero Entry Node.
- Il nodo conosce l'indirizzo IP da cui proviene il messaggio ma non può leggere il messaggio originale perché ci sono ancora due livelli di crittografia aggiuntivi.
- Il primo nodo invia il messaggio al Middle Relay che rimuove il secondo livello di crittografia ed inoltra il messaggio al Exit Node.
- Il nodo di uscita rimuove il livello finale di crittografia ed è quello che ha modo di connettersi con l'internet pubblica in modo di inoltrare al destinatario il messaggio.

TOR CIRCUIT


The Hidden Wiki
The Hidden Wiki
6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion
Site information for
6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion
Connection secure
Tor Circuit
This browser
Bridge: obfs4 146.57.248.225
United States 69.237.207.60
Sweden 98.128.135.72
Relay
Relay
Relay
6nhmgdp…jqxzqd.onion
New Circuit for this Site
The Hi
Update 07.20
future.
We will list only v3 .onion's in the
Dark web link
http://s4k4ceia
http://6nhmgdp
http://2jwcnpr
http://jgwe5cjq
Commercial li
http://prjd5pml
http://55niksbc
http://s57divisc
http://wbz2lrxh
http://iwggpyxr
http://rfyb5tlhic
http://ajlu6mrc7iwuiwakojrgvvtarotvkvxqosb4psxijgobjhureve4kdqd.onion/ 420prime - Cannabis in dispensary quality from the UK
http://y22arit74fqnnc2pbieq3wqqvkfub6gnlegx3cl6thclos4f7ya7rvad.onion/ Dark Mixer - Anonymous bitcoin mixer
http://ovai7wvp4yj6jl3wbzihypbq657vpape7lggrlah4pl34utwjrpetwid.onion/ VirginBitcoins - Buy freshly mined clean bitcoins
http://hqfld5smkr4b4xrjcco7zotvoqhuuoehjdvoin755iytmpk4sm7cbwad.onion/ Mixabit - Bitcoin mixer
http://jbtb75gqlr57qurikzy2bxxjftzkmanynesmoxbzzcp7qf5t46u7ekqd.onion/ Darkmining - Bitcoin mining with stolen electricity
http://jhi4v5rjly75ggha26cu2eeyfhwvgbde4w6d75vepwxt2zht5sqfhuqd.onion/ Bitcoin Investment Trust - earn 5-9% per week!
http://rxmyl3izgquew65nicavsk6loyyblztng6puq42firpvbe32sefvnbad.onion/ Mobile Store - Best unlocked cell phones vendor
http://vhlehwexxmbnvecbmsk4ormttdvhlhbnyabai4cithvizzaduf3gmayd.onion/ Kamagra 4 Bitcoin - Like Viagra but cheaper


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Ricerche – nelle profondità del web

MOTORI DI RICERCA DEL DEEP WEB

Tra i più noti motori di ricerca troviamo:

- **Ahimia.fi**, uno dei pochi engine che, pur mantenendo una certa elasticità, pone un limite all'indicizzazione dei siti, non accettando quelli con materiale inaccettabile a livello morale;
- **Haystak**, con l'indicizzazione di oltre **1,5 miliardi di pagine** che include più di **260.000 siti Web**, Haystak è il motore di ricerca più ampio nel contesto del Dark Web anche se, rispetto al precedente, risulta ricco anche di attività e informazioni che non hanno nulla a che fare con la legalità;
- **Torch** è invece uno dei decani del settore, visto che è attivo dall'ormai lontano **1996**. Pur non avendo un numero di indicizzazioni paragonabili ad Haystak è facile e veloce da consultare;
- **DuckDuckGo** è un motore di ricerca disponibile a tutti, anche al di fuori del Dark Web, visto che l'engine è liberamente accessibile a chiunque e non presenta particolari rischi.

RICERCHE – NELLE PROFONDITÀ DEL WEB

- L’anonimato e la riservatezza che caratterizzano il deep web, portano gli utenti a utilizzarla per scopi poco trasparenti.
- Una parte dei contenuti presenti all’interno del deep web è rappresentato da attività illegali. Questo tipo di attività forma in una parte specifica del deep web: **il dark web**.
- Nel dark web, ad esempio, possiamo trovare dettagli di carte di credito per pochi dollari. Inoltre, è possibile acquistare documenti di cittadinanza e passaporti falsi o mettersi in contatto con sicari professionisti.

Da dato a valore economico

Il valore del Dato

- La possibilità di accedere e copiare dati in rete, dovute a livelli di sicurezza inadeguati, ha prodotto negli anni le prime "raccolte" di informazioni pubblicate nel dark web
- Evoluzione dello spionaggio industriale, furto di brevetti, ecc…
- Il dato diventa merce di scambio monetizzata
- Si aprono mercati di scambio dati ma anche richieste di riscatto per dati prelevati

MODELLI DI MERCATI NERI

- L'economia sotterranea del crimine informatico è estremamente vasta e spesso la sua dimensione e struttura è difficile da comprendere.
- A partire dal gennaio 2016, si stima che i cripto-mercati abbiano generato un volume di denaro mensile che si attesta tra 14,2 e i 25 milioni di dollari americani.
- I mercati delle Darknet consentono i pagamenti attraverso cripto-valute offuscando le transazioni, specialmente con l'uso negli ultimi anni di Monero e Zcash.

PRODOTTI E SERVIZI

- Droga
- Falso Documentale
- Banconote false e carte di credito
- Armi
- Malware e altri strumenti di hacking

Ransomware

RANSOMWARE

- Tipo di malware per cifrare i dati con una chiave segreta e chiedere il pagamento di un "riscatto" per renderli nuovamente usufruibili
- Primi esperimenti dagli anni 90
- Si stima che il costo medio totale di recupero da ransomware sia più che raddoppiato nel 2021 rispetto al 2020 (da 761.106 dollari del 2020 a 1.85 milioni di dollari nel 2021)
- WannaCry, CryptoLocker, NotPetya, ….

RANSOMWARE


PETYA RANSOMWARE
Start
Payment
FAQ
Support
English
Your computer has been encrypted
The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.
The price will be doubled in:
6 days 13 hours 43 minutes 10 seconds
Start the decryption process

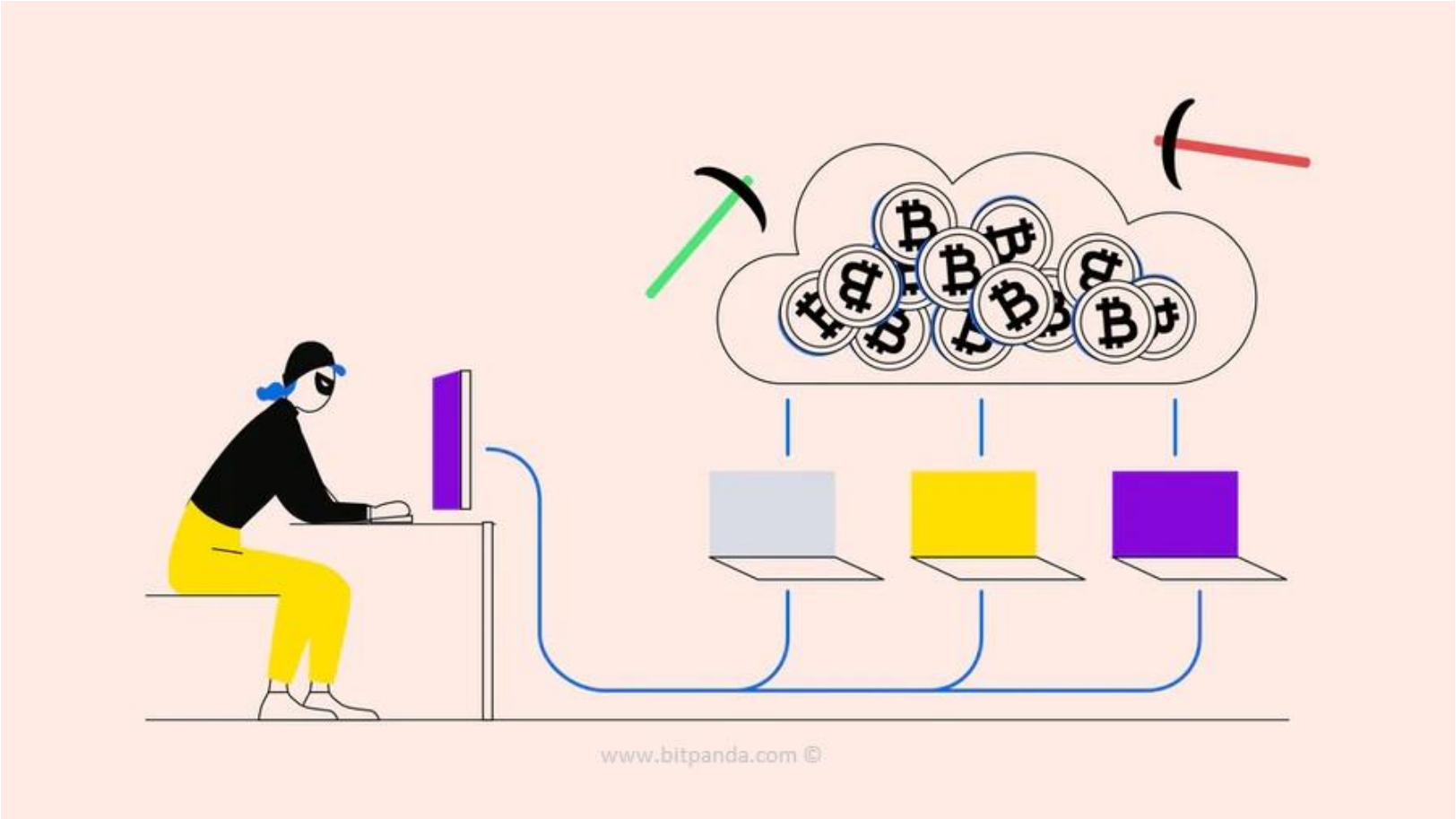

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
2:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
05:23:57:37
About bitcoin
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

Cryptomining

CryptoMining

- Il termine **mining** deriva dall'inglese *to mine*, che significa estrarre, e nel caso di criptovaluta si ottiene attraverso un **processo di condivisione della potenza di calcolo degli hardware dei partecipanti alla rete**.
- Il mining è un'attività estremamente costosa e complessa, sia in termini di CPU che di consumo di energia elettrica.

CRYPTOJACKING



CRYPTOJACKING

- Il cryptojacking (anche chiamato cryptomining dannoso) è una minaccia online emergente, che si nasconde su un computer o dispositivo mobile e utilizza le risorse della macchina per "generare" tipi di denaro virtuale noti come criptovalute.
- La maggior parte dei software di cryptojacking è progettata per rimanere nascosta, ma questo non significa che non ci siano delle conseguenze. Il furto delle risorse di elaborazione rallenta gli altri processi, aumenta le bollette dell'elettricità e riduce la vita utile del dispositivo.

CRYPTOJACKING

I cryptojacker possono sfruttare un computer in vari modi.

- Uno dei metodi è simile a quello utilizzato dai malware classici. Facendo clic su un link dannoso in un'e-mail, il codice di cryptomining viene caricato direttamente sul computer. Una volta che il computer è stato infettato, il cryptojacker inizia a lavorare per generare criptovalute, rimanendo in background.
- Un approccio alternativo al cryptojacking è quello talvolta denominato "drive-by cryptomining". Come per gli exploit pubblicitari dannosi, questo metodo prevede l'integrazione di un codice JavaScript in una pagina web. Dopodiché, inizia la generazione di criptovalute sulle macchine che visitano la pagina.

Grazie .....