15/04/2026

Academy Scuola di Perfezionamento Ingegneria ASTM

Progettazione, costruzione e gestione del patrimonio infrastrutturale: la gestione del rischio e la cyber security

G.Manzini

ITINERA
ASTM GROUP

Indice

Cyber

Surface Web vs. Deep web vs. Dark Web 3

Dark Web 4

Il Raas nel Dark 5

Ingegneria sociale 6

Il cyber diventa fisico 7

Conclusioni 8

SURFACE WEB vs. DEEP WEB vs. DARK WEB

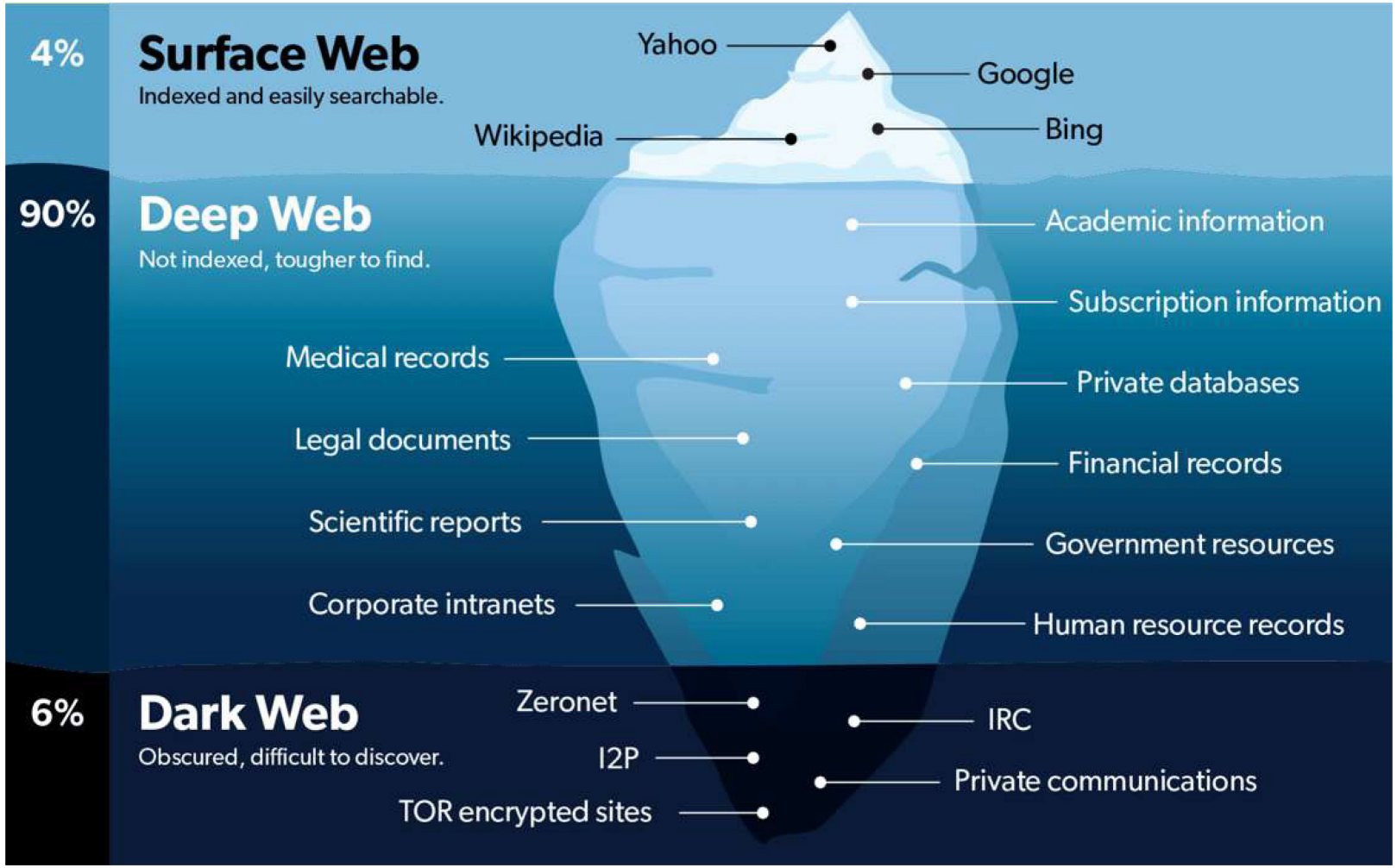
Con Surface Web identifichiamo la parte internet che è facilmente accessibile durante una ricerca

Deep Web indica la parte di Internet che non è Indicizzata dai motori di ricerca
Non inaccessibile — solo invisibile a chi non sa cercare.

I Google Dorks sono operatori avanzati che permettono di trovare nel Deep Web documenti riservati, database esposti e accessi lasciati aperti senza alcun software speciale.
Es: site:<site> filetype:pdf

Il darkweb è intenzionalmente nascosto ed è possibile accederci solo attraverso specifici software

Non è solo il luogo dei criminali è il luogo dove i criminali fanno affari. Credenziali aziendali, accessi VPN, dati di progetto: tutto ha un prezzo, tutto ha un mercato.



DARK WEB

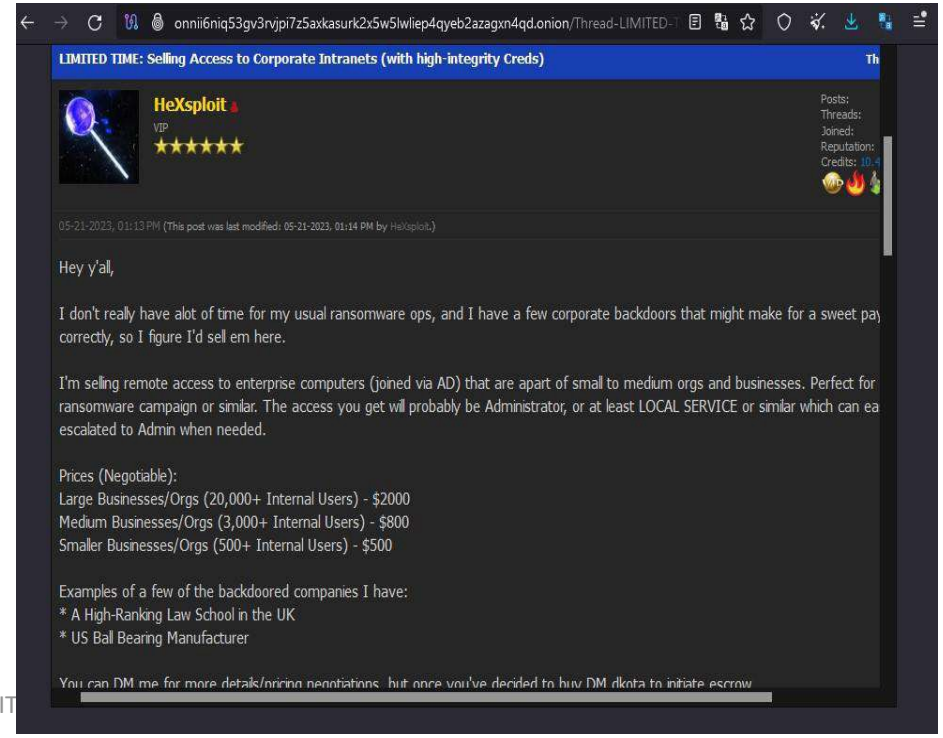
Come si naviga nel Dark, di cosa abbiamo bisogno?

- **Con un browser sicuro e anonimo, il più famoso è TOR (the onion router)**
- **Onion link: è un indirizzo web utilizzato per accedere a siti e servizi web situati nel TOR network**
- **Tanta attenzione: è importante essere molto cauti! I rischi legali e di sicurezza sono reali**

TorProject.org

Le due anime del Dark Web

Non è solo il luogo dei criminali — è il luogo dove i criminali fanno affari. Credenziali aziendali, accessi VPN, dati di progetto: tutto ha un prezzo, tutto ha un mercato.



Il Dark Web nasce come estensione radicale di un principio fondante di internet: la libertà di comunicare senza intermediari. È un internet peer-to-peer, dove nessun governo, nessuna azienda e nessun algoritmo decide cosa puoi leggere o con chi puoi parlare.

- **Washington Post pubblica una versione gratuita sul Dark Web accessibile a chiunque, anche dove la stampa libera è vietata**
- **Whistleblower e giornalisti usano TOR per comunicare in sicurezza**
- **Dissidenti politici in regimi autoritari lo usano per organizzarsi e informarsi**
- **SecureDrop usato da NYT, Guardian, BBC per ricevere documenti riservati in modo anonimo**
- **WikiLeaks: non un singolo whistleblower, ma la piattaforma ha usato TOR come infrastruttura per ricevere documenti in modo anonimo da diverse fonti nel corso degli anni.**

Il RaaS nel Dark

Con Software as a Service si identifica il modello di erogazione tramite Cloud di software e di servizi

Nel Dark: RaaS - Ransomware as a Service

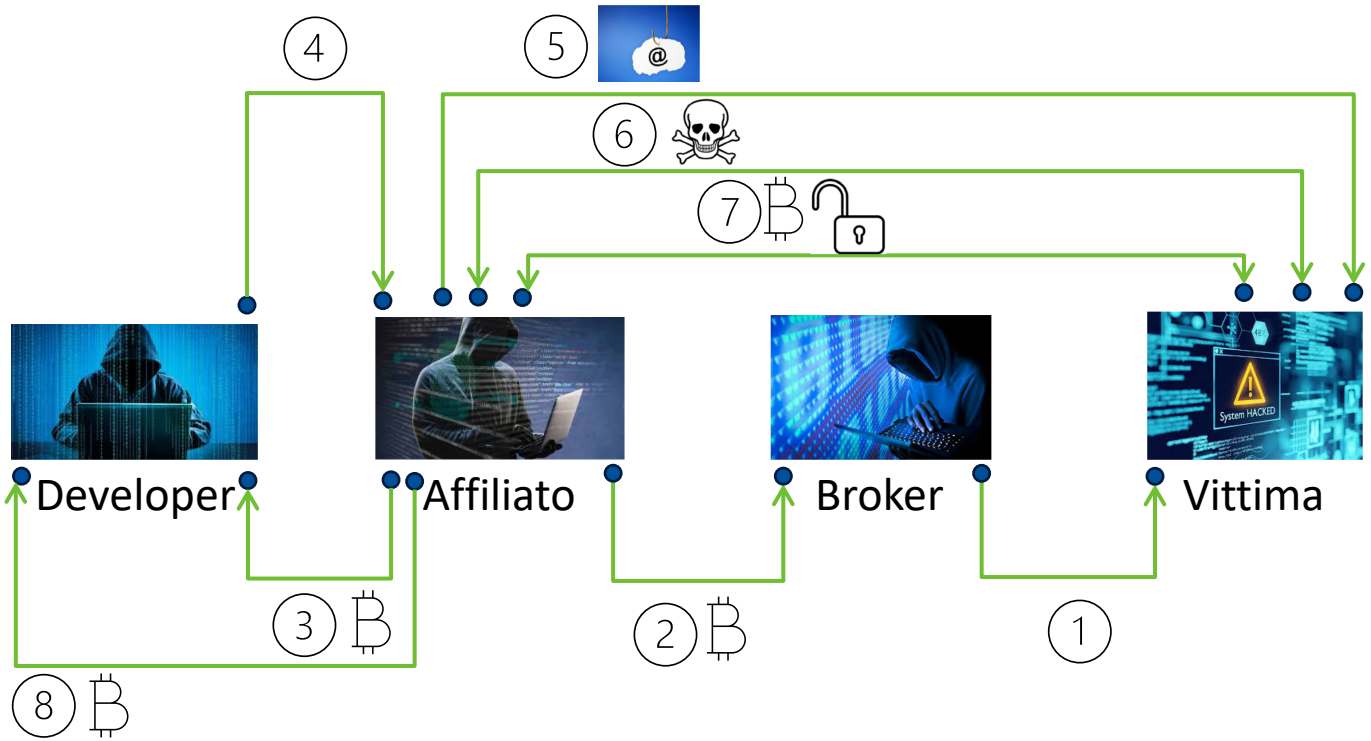
E' un modello di business usato dagli sviluppatori di Ransomware per offrire agli utilizzatori, anche inesperti (Script Kiddie… skiddie) prodotti e kit capaci di lanciare attacchi di questo tipo

Sviluppatori: professionisti che hanno la capacità di scrivere Ransomware

Affiliati: sfruttano il servizio e conducono l'attacco

Broker: forniscono le informazioni di accesso al target

Le vittime: aziende, enti pubblici che subiscono l'attacco informatico



Ingegneria sociale

Kevin David Mitnick
n. 6 agosto 1963 — Van Nuys, California
m. 16 luglio 2023 — Las Vegas
Autore di The Art of Deception — il manuale dell'ingegneria sociale.

- **Fondatore nel 2003 e poi CEO di Mitnick Security Consulting**
- **Clienti: governi, multinazionali**
- **Settori: Finance, Tech, Difesa**
- **Servizi offerti: Penetration testing, Social engineering, Red teaming**

CONDOR, la storia:
Detenzione per circa 5 anni: una prima una condanna nel 1988, poi la più famosa dal 1995 al 2000, di cui 8 mesi in isolamento. (Federal Correctional Institution Lompoc, California).
Il giudice era talmente spaventato dal suo mito da convincersi che Mitnick fosse in grado di scatenare una guerra nucleare fischiettando un codice al telefono al NORAD. Scontata la pena per 3 anni gli fu vietato di usare computer e cellulari

Cosa ha fatto:
Considerato il più famoso hacker della storia, Condor non era un programmatore geniale ma era un manipolatore straordinario. Riusciva ad entrare nei sistemi più protetti del mondo semplicemente telefonando, fingendo identità false e convincendo le persone a dargli accesso. Nessun malware solo psicologia. Tra i suoi bersagli: Nokia, Motorola, Sun Microsystems, Pacific Bell e il Pentagono…. gli stessi che poi ha difeso con la Mitnick Security Consulting.

Cos'è l'ingegneria sociale

Non attacca i sistemi. Attacca le persone

I principi su cui si basa:
Fiducia — si finge di essere qualcuno di legittimo: un collega, il supporto IT, un fornitore
Autorità — si usa un tono autorevole per non essere messi in discussione (*"Sono il responsabile IT, ho bisogno delle sue credenziali"*)
Urgenza — si crea pressione temporale per impedire di ragionare (*"Se non lo fa adesso il sistema va giù"*)
Paura — si minaccia una conseguenza negativa per spingere all'azione
Reciprocità — si fa un favore prima di chiedere qualcosa in cambio

Le forme più comuni oggi:
Phishing — email che imitano mittenti legittimi
Vishing — la stessa cosa al telefono (come faceva Mitnick)
Pretexting — costruire una storia credibile per ottenere accesso
Baiting — lasciare una chiavetta USB in un parcheggio aziendale e aspettare che qualcuno la inserisca

"Ho sempre usato la porta principale. Me la aprivano loro."

Il cyber diventa fisico

L’attacco parte dall’uomo, dalla fiducia, dal telefono (Condor)

L’attacco si industrializza, scala, diventa un servizio (Raas)

L'attacco non colpisce più solo i dati, colpisce il mondo fisico… IoT / OT

Stuxnet (2010): Il primo attacco nella storia che ha distrutto fisicamente un impianto. Un malware progettato da USA e Israele ha infettato le centrifughe nucleari iraniane di Natanz facendole girare fuori controllo fino a rompersi — mentre i monitor mostravano tutto normale. Nessun esplosivo, nessun bombardamento. Solo codice.

Nessuna cifra ufficiale
Circa 1.000 centrifughe distrutte..
Lo sviluppo del SW è stimato oltre 1 bln $

Il nome non è mai stato reso pubblico. Fonte: BSI, agenzia governativa tedesca per la cybersecurity.

Acciaieria tedesca (2014): Attacco tramite phishing sulla rete aziendale, poi pivot sulla rete OT. Risultato: impossibile spegnere correttamente l'altoforno. Danni fisici ingenti all'impianto.

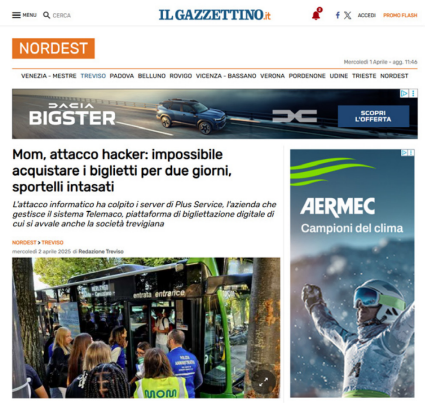
Nessuna cifra ufficiale

Colonial Pipeline (2021): Ransomware sulla rete IT: i sistemi OT non furono direttamente colpiti, ma l'azienda fermò tutto preventivamente. Risultato: blocco della fornitura di carburante all'intero sud-est degli Stati Uniti per giorni, file ai distributori, stato di emergenza dichiarato.

Riscatto pagato:
4,4 milioni $ in criptovaluta.
Oleodotto fermo per 4 giorni. 5.500 miglia di pipeline bloccati.
Danno economia americana stimato in miliardi

Oldsmar, Florida (2021): Un attaccante entrò da remoto nel sistema di controllo di un impianto idrico e tentò di aumentare il cloro nell'acqua potabile a livelli letali. Fu fermato per caso da un operatore che vide il cursore muoversi da solo.

Nessuna cifra ufficiale.
Nessun danno economico — l'attacco fu sventato per caso. Il danno potenziale era la contaminazione dell'acqua potabile di circa 15.000 persone



Italia (2025): Attacco supply chain su Plus Service: biglietteria MOM (mobilità di marca) Treviso bloccata per 2 giorni. Oltre 150 aziende di trasporto coinvolte. Nessuna cifra ufficiale: né il riscatto pagato, né il costo di ripristino.

Conclusioni

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Eugene "Gene" Spafford
professor of computer science at Purdue University
Scientific American marzo 1989

BEHIND THE JOURNEY
BEYOND THE DESTINATION