UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Dentro la rete che (non) vediamo: Dark Web e Privacy

Chiara Mariotti

Giovedì 2 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

"La rete ha tante ombre, ma la luce siamo noi se sappiamo dove guardare"

Sammy Basso

Il vero volto di internet

🌐 **Surface Web**: il web in chiaro. Si tratta di tutte le pagine accessibili liberamente tramite una normale connessione e facilmente individuabili dai motori di ricerca (Google, Bing, ecc.).

🔒 Appena sotto il livello dell'acqua si trova il **Deep Web**. È l'insieme di contenuti non indicizzati, cioè non raggiungibili tramite i motori di ricerca. La maggior parte di questi contenuti è legittima, ma una piccola parte viene utilizzata per scopi illeciti: conoscendo direttamente l'indirizzo, diventa comunque accessibile.

🕶️ Ancora più in profondità c'è il **Dark Web**, la porzione più nascosta e inaccessibile dell'iceberg. Per accedervi servono degli strumenti specifici, progettati per garantire l'anonimato sia degli utenti sia dei server. Il più diffuso è **Tor (The Onion Router)**, che permette di collegarsi a reti particolari chiamate **darknet**. La più conosciuta è proprio la rete **Onion**, dove si trovano i siti tipici del Dark Web.

Le tecnologie dell’anonimato

- TOR (THE ONION ROUTER) --> Crittografia a più strati (onion routing) per nascondere l'identità
- PSEUDONIMIZZAZIONE VS. ANONIMIZZAZIONE --> La pseudonimizzazione sostituisce i dati sensibili ma può essere reversibile (GDPR). L'anonimizzazione rende i dati irreversibilmente anonimi.
- ESEMPIO DI RI-IDENTIFICAZIONE --> Il caso del governatore del Massachusetts dimostra come dati pseudonimi e pubblici possano essere correlati per esporre la privacy.

Le due facce del Dark Web

Usi Legittimi

- Protezione della libertà di espressione → è un rifugio per whistleblower, giornalisti e attivisti in paesi con regimi repressivi.
- Aggirare la censura → Anche Facebook ha creato una versione «onion» che permette agli iscritti di accedere in maniera anonima e sicura alle informazioni aggirando i sistemi di filtraggio.

Ambiente criminogeno

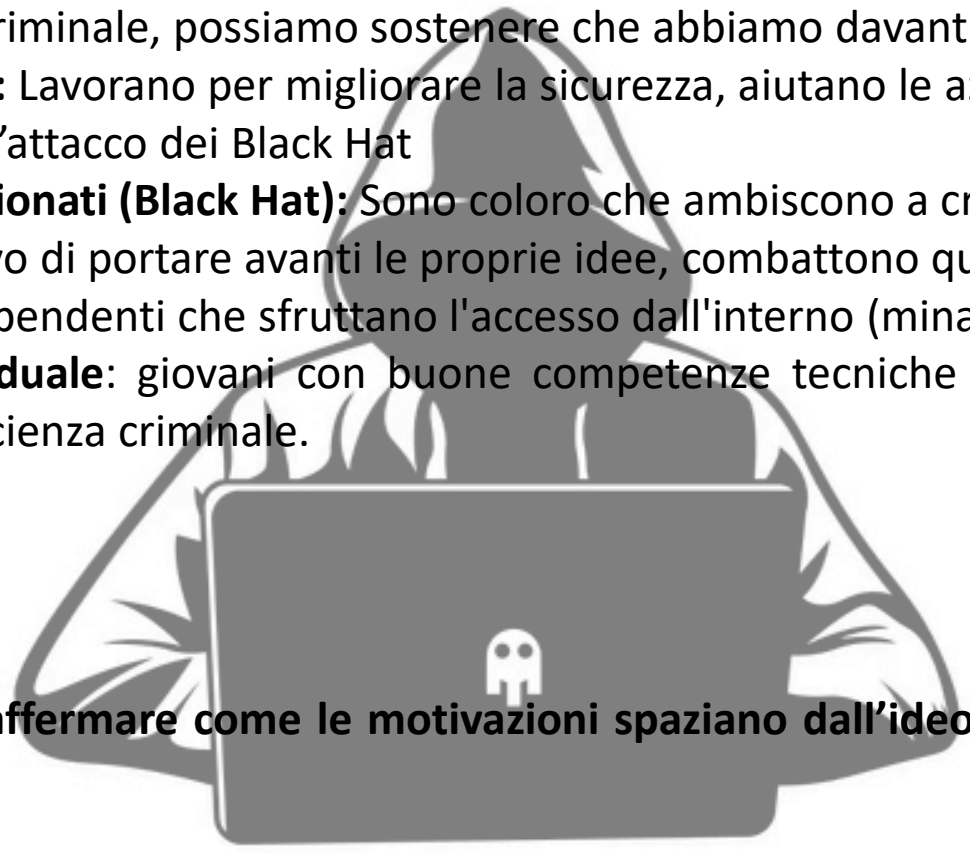
Usi Illegittimi

- Mercato nero per beni e servizi illegali → droghe, merce contraffatta, documenti falsi, armi
- Hub (luogo) per il cybercrime → è proprio qui che si vendono e organizzano gli attacchi informatici, degli esempi possono essere le frodi e i furti di dati. Questo significa che i dati non vengono rubati dal dark web ma su delle piattaforme legittime; il DW è solamente il luogo dove le informazioni vengono vendute a seguito degli attacchi.
- Traffico di dati personali → nomi, indirizzi, codici fiscali messi in vendita anche solo a 5 centesimi

Il Profilo del Cybercriminale

Quando parliamo di Cybercriminale, possiamo sostenere che abbiamo davanti diverse tipologie di attori:

- **Hacker etici (White Hat):** Lavorano per migliorare la sicurezza, aiutano le aziende e le organizzazioni a correggere i loro punti deboli per evitare l'attacco dei Black Hat
    - **Hacker malintenzionati (Black Hat):** Sono coloro che ambiscono a creare danno per guadagnarci sopra.
- **Hacktivisti:** Con l'obiettivo di portare avanti le proprie idee, combattono quelle che ritengono ingiustizie sociali.
    - **Insider Threat:** Dipendenti che sfruttano l'accesso dall'interno (minacce interne).
- **Devianza digitale individuale**: giovani con buone competenze tecniche che sperimentano forme di "trasgressione online", senza una vera coscienza criminale.



Possiamo di conseguenza affermare come le motivazioni spaziano dall'ideologia al guadagno passando per il senso di sfida.

L’industrializzazione del crimine

Ransomware-as-a-Service (RaaS) → È un modello di business criminale in cui i creatori di ransomware affittano i loro "kit" a criminali meno esperti, abbassando la barriera d'ingresso al cybercrime.
Un attacco ransomware compromette **l'integrità**, **la disponibilità** e **la riservatezza** dei dati aziendali, causando così dei danni. (art. 5 GDPR)
Ci sono 4 tecniche di estorsione che mettono in atto i criminali per obbligare le vittime a pagare:

- **Cifratura dei dati:** Bloccano l'accesso ai file aziendali.
- **Pubblicazione dei dati:** Pubblicano gradualmente i dati rubati sul dark web per danneggiare la reputazione e far scattare sanzioni (nb obbligo di notifica e sanzioni per non avere implementato la sicurezza).
- **Attacco DDoS (**Distributed Denial of Service**):** Rendono i servizi web dell'azienda indisponibili e ciò comporta la perdita di controllo dei dati e dei servizi che quest’ultima offrirebbe.
- **Minacce ai contatti:** Contattano clienti, fornitori o dipendenti per minacciare la divulgazione di dati personali.

Anche l’Italia ha subito diversi attacchi ransomware, posizionandosi al quinto posto per attacchi subiti.

La violazione della Privacy

- Il problema reale non è il Dark Web, ma il Data Breach «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» Art. 4, n. 12, GDPR

- I dati personali vengono rubati da piattaforme legittime tramite attacchi su larga scala (data breach) e attacchi mirati (phishing: sono delle strategie psicologiche pensate per ingannare la vittima e indurla a compiere azioni pericolose, come cliccare su un link, scaricare un allegato o fornire le proprie credenziali).
- Questi furti violano direttamente il GDPR e, a volte, le aziende usano delle pratiche ingannevoli «dark patterns» per farti acconsentire alla raccolta di più dati del necessario.

https://www.garanteprivacy.it/temi/internet-e-nuove-tecnologie/dark-pattern)

Quando l’anello più debole è l’uomo

Il fattore umano è da sempre considerato l’anello più debole della catena della sicurezza e per questo gli attaccanti investono principalmente in tecniche che colpiscono non direttamente in sistemi informatici ma le persone che li utilizzano.

Sono strategie psicologiche che ingannano la vittima portandola a compiere azioni pericolose, come cliccare su un link oppure fornire le proprie credenziali. La tecnica più diffusa è quindi il phishing e, anche la tecnica Honeytrap, in cui l’attaccante costruisce una relazione fittizia per manipolare la vittima.

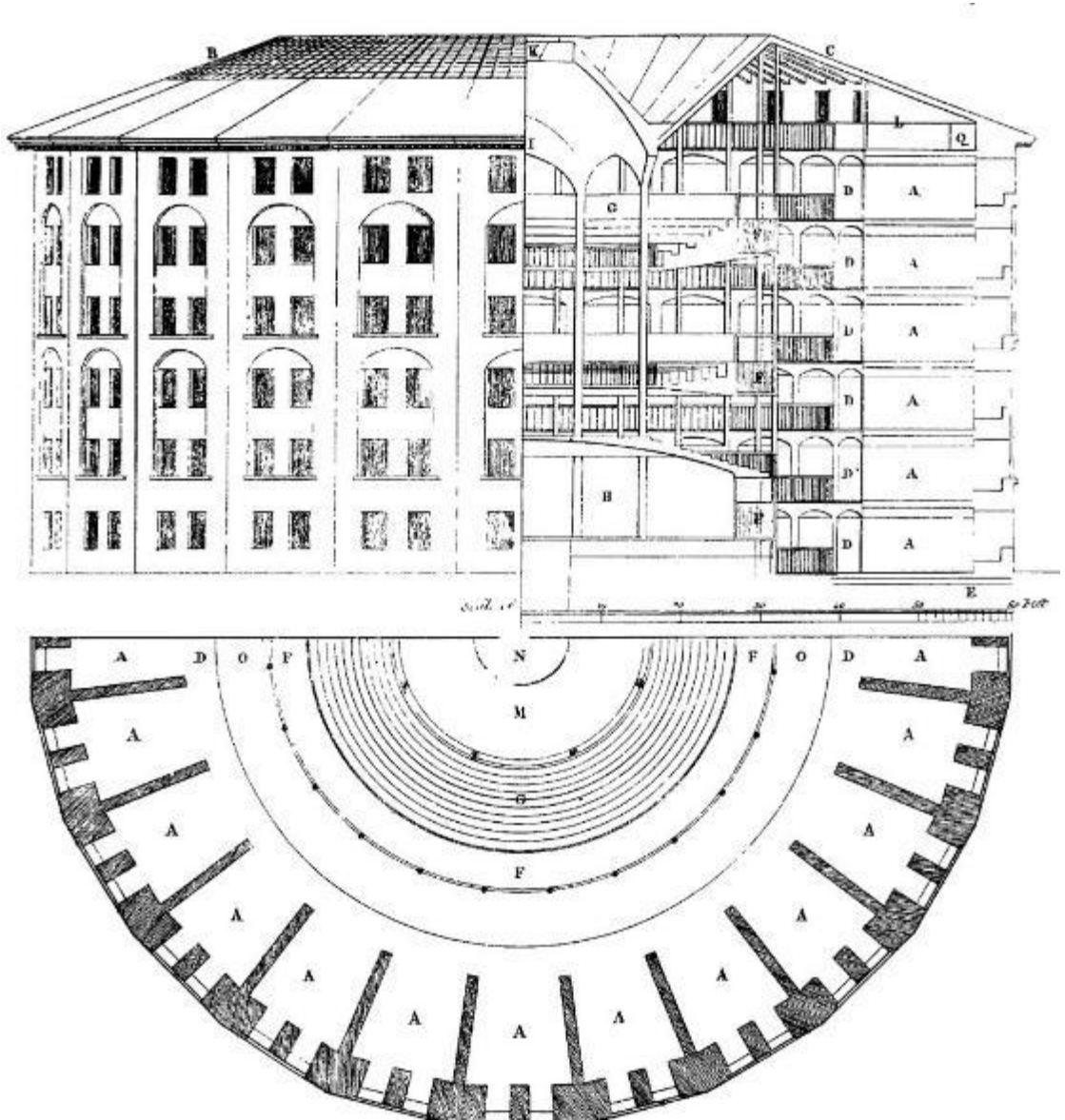
La tecnologia protegge, la consapevolezza difende.

Criptovalute: anonime o pseudonime?

Le criptovalute sono strettamente legate al successo dei mercati neri del Dark web.
Differentemente da quanto è stato percepito negli anni, esse non sono uno strumento di pagamento anonimo ma pseudonimo perché ogni transazione viene in realtà registrata su un registro pubblico, **la blockchain** che permette, tramite l'analisi forense, di tracciare i flussi di denaro e risalire agli autori dei reati → SILKROAD, La via della seta

Tra tutela e controllo: Privacy e Sorveglianza

Modello Panottico Digitale: applicazione del concetto di Jeremy Bentham e Michel Foucault.



Il quadro normativo

⚖️ **Nuove normative** per affrontare il Dark Web

🤖 trasparenza su contenuti generati da AI (deepfake) → Ai Act

📊 più controllo ai cittadini sui dati → Data Act

🌍 anonimato e assenza di confini

Conclusioni

Il Dark Web rappresenta sia l’esigenza di riservatezza e sia il terreno fertile per il crimine.

I cittadini sono esposti a rischi anche sulle piattaforme considerate legittime.

Il crimine informatico si è industrializzato e globalizzato.

Per proteggere la sicurezza digitale, serve un approccio globale: tecnologia, normativa e consapevolezza.

Grazie per l'attenzione

Chiara Mariotti

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection