UNIONE POLIZIA LOCALE ITALIANA
Articolo disponibile all'indirizzo: www.unionepolizialocaleitaliana.it/2021-15/

I RISCHI OSCURI DEL DARK WEB

di Laura Crapanzano [a]

ABSTRACT: *Una breve guida schematica al mondo profondo (deep web) e oscuro (dark web) della rete internet, che viaggia parallelamente ai canali superficiali, celando traffici illeciti di ogni genere, crimini anche efferati, e tanti, tanti rischi, rendendo disponibile a tutti una terra di mezzo fuori dai controlli e difficile, se non impossibile, da intercettare e reprimere.*

KEYWORDS: #darkweb #deepweb #tor #telegram #hacking #phishing #criminalitàinformatica #lauracrapanzano #EspertiUPLI #UPLI #UnionePoliziaLocaleItaliana.

INDICE

IL META WEB OSCURO

Una delle più gravi e pericolose trappole del web di cui i nostri figli, smanettoni, in special modo in questo periodo di pandemia per il sars-cov-2, obbligati a restare a casa, grazie alla DAD, e alla solitudine si avvicinano, spesso inconsapevoli di quello che possono trovare e nelle situazioni gravi che possono incorrere.

Iniziamo con il dire che il web, i link e tutto quello che noi consociamo ed è visibile nelle nostre ricerche è come una piramide rovesciata, noi vediamo solo la punta ma sotto si aprono due grandi mondi, il mondo del deep web, e quello più pericoloso , terrificante ed esecrabile il deep web.

Sia sul web che sul deep web si può navigare anonimamente e questo non vuol dire per forza voler fare qualcosa di illegale, poiché non c'è alcuna norma che lo vieta e, di per sé, questo comportamento non costituisce necessariamente il presupposto per compiere crimini.

IL TRACCIAMENTO DEGLI ACCESSI SUL WEB

Normalmente, tutti i nostri movimenti attraverso i browser web più diffusi, come per esempio Firefox e Chrome, sono tracciabili e tracciati, innanzitutto attraverso i cookie, che aiutano gli utenti a reperire alcune informazioni, come per esempio la cronologia di navigazione, e aiutano i marketers a proporre annunci e promozioni aderenti alle esigenze del loro target di riferimento.

Poi c'è il controllo di tutte le attività legate alla gestione e supervisione del traffico di rete e dei flussi di dati degli indirizzi IP, come fanno i sistemisti di rete e gli addetti Al CED che possono vedere quali siti visitano e quali azioni compiono gli utenti della rete aziendale.

Allo stesso modo potrebbe farlo il fornitore dei servizi web, quindi se si visita un sito con contenuti illegali, si è facilmente individuabili e può avvenire facilmente la divulgazione non autorizzata dei dati personali.

---

[a] *Presidente nazionale UPLI, criminologa, operatrice della Polizia Locale Massa, DPO/RPD e consulente privacy in enti pubblici e aziende private esperto in DPIA.*

DEEP E DARK WEB

Il termine deep web, [traduzione letterale: web profondo] è usato per distinguere il surface web [traduzione letterale: web superficiale] o web accessibile[1], è una sostanziosa parte di internet non indicizzata nei motori di ricerca standard.

Ci si può accedere quindi attraverso indirizzi IP o URL diretti e possono essere richieste password o altri strumenti di sicurezza per proseguire oltre la pagina pubblica del sito.

Il dark web [traduzione letterale: web oscuro] è un componente del deep web che descrive la più ampia gamma di contenuti che non appare attraverso le normali attività di navigazione in internet e necessita di browser specifici, come ad esempio Tor, per la sua navigazione.

Questa "area sommersa" comprende molto comunemente web mail, banking online, pagine e profili di social media privati o comunque ad accesso riservato, forum online che richiedono un'iscrizione per visualizzarne i contenuti e servizi che richiedono un pagamento da parte dell'utente, come video on-demand e riviste o giornali online, personalizzati per gli utenti e per questo non destinati ad essere indicizzati.

Il browser TOR[2], acronimo di The Onion Router, è un software libero, rilasciato su licenza BSD, con un'interfaccia di gestione disponibile che permette una comunicazione anonima per Internet basata sulla seconda generazione del protocollo di rete di onion routing, tramite il suo utilizzo è molto più difficile tracciare l'attività Internet dell'utente poiché utilizza piccole reti friend-to-friend di tipo peer-to-peer, dove cioè i nodi sono paritari e pertanto fungono contemporaneamente da client e server verso gli altri nodi della rete.

LE RETI CLANDESTINE

Le dark net possono essere utilizzate per vari motivi tra i quali: condivisione di file piratati, personali, illegali o contraffatti, etc.; crimini informatici come hacking, corruzione di file, frodi, etc.; vendita di beni limitati su mercati, fra cui droghe e sostanze psicotrope, farmaci chemioterapici, doping; compravendita di beni o servizi illeciti o illegali come sostanze stupefacenti, armi, reclutamento per il terrorismo e crimini vari; whistleblowing[3], ossia le segnalazioni di attività illecite o fraudolente all'interno del governo; fughe di notizie per fini di spionaggio, dossieraggio, giornalismo investigativo; traffico di materiale pedopornografico; vendita di organi umani; assoldare killer; ma la cosa più terribile è che ci sono dei siti in cui le persone possono interagire, dietro pagamento, a mutilazioni sino alla morte oppure a violenze incredibili sino all'omicidio di vittime sacrificali fra le quali anche neonati.

Per accedervi, c'è bisogno di software specifici o configurazioni particolari di reti, come la rete Tor di cui si è già detto, alla quale si accede mediante l'omonimo browser o attraverso server proxy.

---

[1] https://it.wikipedia.org/wiki/Web_sommerso

[2] https://it.vpnmentor.com/blog/tor-browser-cose-come-funziona-e-cosha-che-fare-con-il-mondo-vpn/

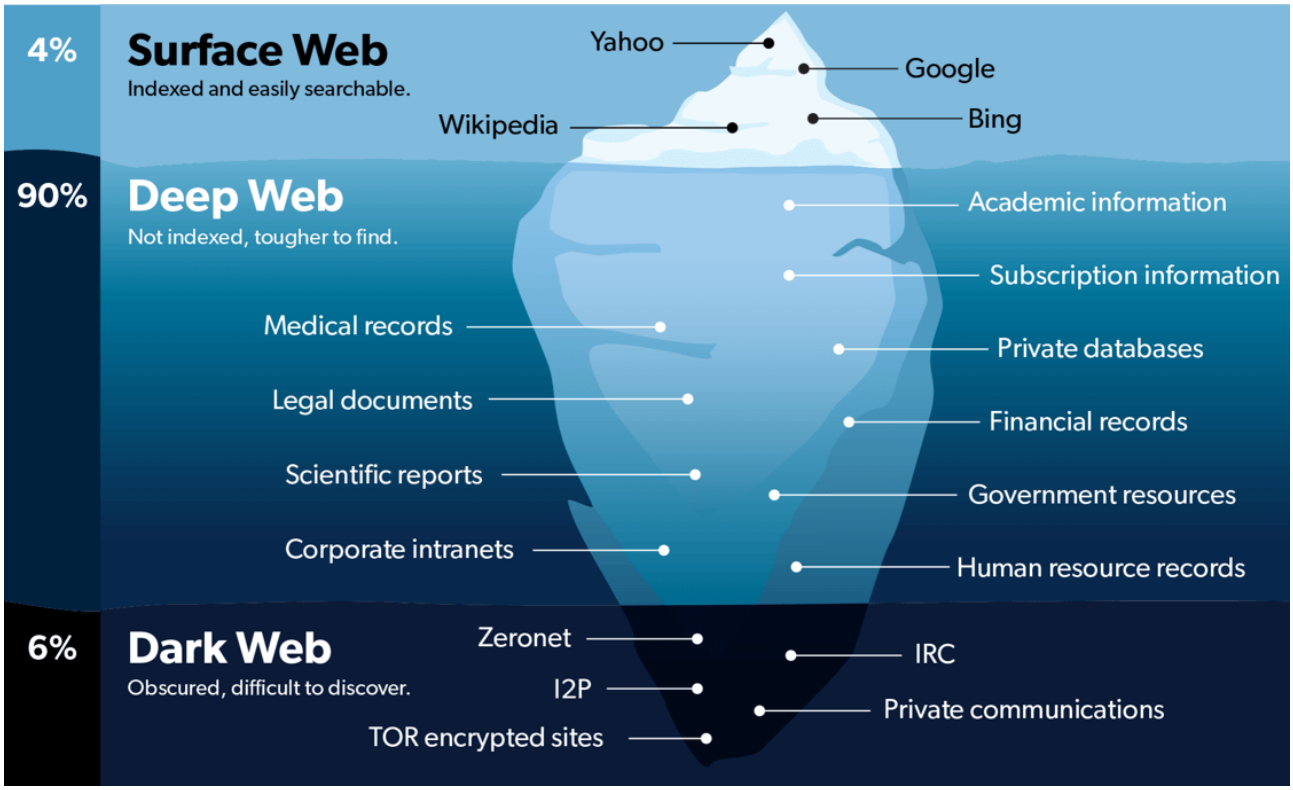
[3]https://www.isweb.it/wb-landing?gclid=CjwKCAiAjp6BBhAIEiwAkO9Wuu7_jZYyEkRbpjbKCBFzfwSj8Wr8_yIgPkCmfVtYJnO4FOAWpmwYxxoCORoQAvD_BwE

La stessa app Telegram, per le sue caratteristiche di sicurezza crittografica e per aggirare il divieto imposto a questa applicazione sul territorio della Russia e di altri paesi, appartiene alla dark net.

Nel dark web, le informazioni vengono ulteriormente scomposte e fatte rimbalzare prima di arrivare a destinazione.

Tutti i punti, ossia i nodi, in cui transitano i pacchetti di dati, possono disporre solo di due informazioni[4]: l'indirizzo del precedente nodo da cui arriva il pacchetto e quello del successivo a cui devono trasmetterlo, quindi non conoscono l'identità del mittente e del destinatario.

Se le autorità intercettano uno di questi pacchetti non possono utilizzarlo, anche perché in ogni passaggio le informazioni vengono criptate con un sistema di cifratura diverso per ogni nodo della rete.



[4] https://www.tecnisoft.it/ziplist/Manuale.pdf