Di recente sul blog di Kaspersky è apparso un interessante articolo di Leonid Grustniy che fa chiarezza sulla terminologia dei tipi di Web (How the darknet, dark web, deep web, and surface web differ | Kaspersky official blog). L'articolo è semplice e interessante e ne offriamo qui una versione tradotta in italiano.

Cosa vi fa venire in mente il termine "deep web"? Un luogo per hackers semidivini dove i miseri mortali devono temere ad avventurarsi? Un covo di malvagità? Se fosse così potrebbe sorprendervi sapere che utilizzate il deep web ogni singolo giorno.
Infatti, poiché il termine *deep web* è facilmente confuso con i termini simili *dark web* e *darknet* (come successe anche al film documentario Deep Web, che trattava del dark web), pensiamo che meriti fare un po' di chiarezza sulla questione.

Deep web e surface web

Utilizzando un'immagine, pensiamo a Internet come ad una grande città. Come in ogni metropoli ci sono spazi aperti a tutti: strade, viali e parchi che si possono trovare su una mappa. Tutti possono andarci e guardarsi attorno; le telecamere a 360° possono riprenderli e potete facilmente ritrovarli su MapQuest o Google Maps.
Dentro Internet questi spazi pubblici sono noti come *surface web* ("web di superfice"). Sono pagine Web, applicazioni e altri elementi che i bot di ricerca - ossia i programmi automatici che sono l'analogo digitale delle videocamere dei cartografi - possono trovare ed indicizzare. Questi spazi possono contenere documenti, musica, video, immagini e molto altro. Tutti possono trovarli usando un motore di ricerca e consultarli senza pagare, registrarsi o installare dei software particolari.
In aggiunta alle aree pubbliche, le città possiedono zone private che richiedono per l'accesso un permesso, un biglietto o un invito. Queste sono ad esempio le case, gli uffici, I club privati, i cinema e così via. Solitamente nessuna mappa pubblica vi mostrerà che cosa accade all'interno di queste aree.
Anche il Web contiene molti luoghi che Google, Bing e altri non possono osservare. Tutti insieme questi luoghi sono noti come *deep web* ("web profondo"). Sono composti innanzitutto da tutte le pagine web che non possono venire ricercate e aperte come le altre e che i bot-cartografi non possono indicizzare.
Se un sito vi richiede di inserire un CAPTCHA per l'ingresso [sequenze di lettere e numeri casuali visualizzate distorte, che solo gli esseri umani possono riconoscere, N.D.T.] allora un bot di ricerca non sarà in grado di capire molto sui suoi contenuti: il CAPTCHA serve proprio a tenere alla larga i bot, dopotutto. Se un articolo è disponibile solo su abbonamento, un bot non può leggerlo e indicizzarlo perché i bot non dispongono di credenziali o denaro per l'accesso. Leggere un documento richiede una password? Di nuovo un bot non ha speranza: non può conoscere la password.
Se qualcosa non può essere trovato, anche se può essere aperto senza restrizioni, allora appartiene al deep web. Se configurate Facebook per nascondere il vostro profilo ai motori di ricerca, ad esempio, anche se un bot di ricerca lo raggiunge dovrà necessariamente ignorarlo. Allo stesso modo un motore di ricerca non può elaborare il contenuto che

una pagina Web genera solo quando questa viene aperta e che può variare a seconda di chi la apre. Ad esempio, per vedere certe offerte personalizzate bisogna essere utenti con certe abitudini di navigazione.
Infine, il deep web si riferisce anche a tutti i contenuti che non presentano dei collegamenti nel Web visibile: un bot di ricerca semplicemente non può sapere che tali contenuti esistono, visto che può trovare nuove pagine solo seguendo i collegamenti da pagine già indicizzate. Proprio come un automobile di Google Street View non può entrare in un cortile privato, così i bot di ricerca non possono trovare contenuti senza collegamenti.
Come potete vedere, il grosso del deep web è composto da innocue e utili pagine web che la maggior parte di noi usa regolarmente: non c'è nulla di sbagliato in questo loro rimanere nascoste agli estranei, anzi il contrario.

Dark web e darknet

Sia nelle città come online, la privacy è desiderata non solo dai cittadini onesti ma anche da coloro che cercano di nascondere le loro attività non propriamente legali. Nel mondo reale pensiamo a traffici oscuri che avvengono in bassifondi e quartieri criminali: posti scelti per l'assenza di passanti e non segnalati sulle mappe pubbliche. Indirizzi e posizioni di questi luoghi sono noti ad un numero ristretto di individui, anche se molti sono al corrente della loro esistenza.
Questo è all'incirca il modo in cui operano le *darknets* ("reti oscure"): reti con accessi ristretti per attività discutibili. I nodi di ogni singola darknet (server, computer, router) sono invisibili non solo ai motori di ricerca ma anche - visto l'utilizzo di protocolli di trasferimento dati non standard - alla maggior parte dei browser. Nessun link diretto e nessuna password potrà portare lì un utente ordinario.
Tutte le darknet insieme compongono il *dark web* ("web oscuro"), generalmente ritenuto un covo per personaggi torbidi come trafficanti di droga, venditori di armi, ricattatori e venditori di dati rubati. Molte persone sanno che il dark web esiste, ma pochi sanno come raggiungerlo.
Naturalmente, hacker e criminali non sono le sole persone che necessitano di segretezza: dissidenti, attivisti della libertà di parola, informatori che aiutano giornalisti investigativi e molte altre categorie utilizzano il dark web per evitare le persecuzioni e comunicare in modo anonimo. Alcune persone lo utilizzano anche solo per proteggersi dalla raccolta dei dati online: allo scopo esistono degli strumenti sicuri ed affidabili ma costoro preferiscono un approccio più radicale.

Tutte le sfumature della Internet security

Non è sbagliato che i dati rimangano nascosti in profondità, invisibili a coloro a cui non sono destinati. Se - ad esempio - la corrispondenza di un'azienda fosse rintracciabile attraverso un motore di ricerca, le conseguenze potrebbero essere sgradevoli. È senz'altro meglio proteggere la propria porzione di profondità: credenziali e documenti a cui solo noi dobbiamo aver accesso.

- Usate sempre password robuste e uniche. Se avete troppe credenziali per ricordarle tutte, allora usate un password manager per tenerle sotto controllo.
- Controllate sempre di essere esattamente dove volete prima di inserire le vostre credenziali online. Ad esempio, se l'indirizzo URL della pagina è impreciso o assomiglia ad un cumulo senza senso di lettere e numeri la pagina non è affidabile.
- Concedete l'accesso a documenti riservati solo a coloro che ne hanno reale necessità.
- Evitate il dark web a meno che non abbiate problemi a distinguere un forum di attivisti dei diritti umani da uno per gli hackers.
- Utilizzate una soluzione di sicurezza affidabile che vi protegga dai guai ogni volta che siete online.