Coordinamento Nazionale Informatici

Flash 2013 N. 2

Ministeri – Agenzie Fiscali – Enti Pubblici – Università - Ricerca – Enti ex art. 70

lunedì 28 gennaio 2013

LE RETI PARALLELE AD INTERNET

La darknet o deep web è definita la parte nascosta di Internet.
Una immensa rete parallela ed anonima, dalle dimensioni impressionanti tali da sovrastare l'Internet in chiaro, che conta oggi milioni di frequentatori connessi da ogni parte del pianeta.
Si tratta di una rete alternativa ad Internet, una porzione del web che non viene indicizzata dai motori di ricerca, di fatto un enorme contenitore di informazioni composto di oltre 200.000 siti, raggiungibili e fruibili solo da chi ne conosce l'allocazione attraverso l'utilizzazione di particolari strumenti.
Nel deep web vi sono una quantità di dati disponibili 500 volte superiore rispetto a quella presente sull'Internet convenzionale.
Questa rete nascosta e parallela ad Internet ha conosciuto una grande espansione all'immediato indomani della chiusura da parte delle autorità statunitensi di Megaupload, community frequentata da milioni di utenti che dal più noto tra i portali di file hosting scaricavano opere dell'ingegno tutelate dal copyright.
Spaventati dal pericolo di identificazione in caso di azioni illecite, i web surfer si sono dedicati alla ricerca di ambienti in cui navigare in grado di garantire l'anonimia, fino a trovare nella darknet la risposta alle loro esigenze.
Essa è nata, quindi, come rete anonima utilizzata da dissidenti politici e religiosi oppressi e perseguiti da governi totalitari e dispotici, da chi non poteva far sentire la propria voce perché oppresso o censurato, o come veicolo di comunicazione di attivisti con il resto del mondo in occasione di moti rivoluzionari o disordini sociali come quelli avvenuti recentemente in Iran o in Siria. La darknet è divenuta, invece, oggi una rete parallela, all'interno della quale non vigono regole e non trovano applicazione le leggi.
Insomma, un enorme bazar dell'illegale, una zona franca al cui interno chiunque può contrabbandare ed acquistare di tutto, dalle armi, alle sostanze stupefacenti, ai documenti falsi.
Come è noto, la navigazione online lascia tracce incancellabili, che le autorità deputate alle indagini possono facilmente recuperare, anche in epoca successiva rispetto alla commissione di un reato o di un attacco informatico e diventa quindi estremamente agevole acquisire tutte quelle informazioni che risulteranno poi necessarie ad individuare i responsabili di azioni contra legem.
Il web offre quindi a chi deve svolgere le investigazioni maggiori opportunità di identificare il responsabile di un eventuale reato, anche rispetto a quanto ciò sia possibile nel mondo reale.

tel. 06.3233363 - 06/3203311 Fax 06/3226052
cell. 392.8836544 - email: anipa@anipa.it

Il deep web, invece, è la rete che sovverte il paradigma di cui sopra, rendendo i net user che vi accedono non tracciabili e quindi non individuabili, con tutte le conseguenze che ne derivano rispetto alla consequenziale non applicabilità di alcuna legge nazionale.
Molti utenti gradiscono preservare in fase di navigazione la propria anonimia e decidono di navigare nascondendo la propria identità per legittime ragioni di privacy, per sicurezza personale o anche perché, dovendo commettere delle azioni illecite, intendono garantirsi la non rintracciabilità.
Una soluzione alla quale molti ricorrono è l'utilizzo dei cosiddetti pubblic anonymous, ovvero dei server che fungono da intermediari e quindi da schermo rispetto ai dati allocati sul computer dell'utente.
Il server del sito visitato vede l'indirizzo IP del server proxy anziché quello dell'utente e ne rimane raggirato.
Tor (acronimo di The Onion Routine), è un noto sistema di comunicazione anonima che utilizza la crittografia a strati.
Il progetto Tor ha la finalità di tutelare gli utenti del web dall'analisi del traffico mediante una rete di onion router, gestiti direttamente da volontari, i quali consentono il traffico anonimo in uscita e la concretizzazione di servizi anonimi nascosti.
L'originario e lodevole fine del progetto di garantire il diritto di manifestare il proprio pensiero in situazioni o ambienti nei quali tale esercizio è vietato (a tal proposito si pensi a quegli Stati totalitari come la Cina in cui ancora forte è la censura, soprattutto nei confronti di un mezzo d'informazione quale Internet), può essere delegittimato dall'uso disonesto che molti cybernauti fanno del particolare strumento.
Da un punto di vista strettamente tecnico, nell'ambito della rete Tor, i dati che fanno parte di una comunicazione non passano direttamente dal cliente al server, ma si muovono attraverso i server Tor che si comportano da router dando vita ad un circuito virtuale crittografato.
L'uso della crittografia a strati, espressione dalla quale deriva il vocabolo onion, che in inglese significa cipolla, garantisce la riservatezza dei dati.
Difatti, ciascun onion router stabilisce a quale nodo della rete inviare i pacchetti e negozia una coppia di chiavi crittografiche per spedire i dati in modo sicuro; in tal modo, nessun osservatore, posizionato in un punto qualsiasi del circuito, sarà in grado di monitorare la connessione.
In definitiva le procedure di accesso al web sommerso differiscono quindi dai canoni standard di Internet.
Entrare nella darknet è piuttosto facile e la sola procedura attuabile non postula competenze informatiche da hacker o da utente consumato; detta semplicità di accesso ad un mondo così ricco di fascino, ma allo stesso tempo pericoloso, è uno dei motivi per il quale oggi molti ragazzi ed adolescenti scelgono di navigare nel deep web invece che nel web classico.
Per molti, è qui che è possibile soddisfare la naturale sete di esperienze ed il legittimo desiderio di sperimentare, ma come spesso accade, ad una innata predisposizione e ad una sviluppata manualità nell'utilizzo di device multimediali e del web in generale, non

corrisponde una necessaria conoscenza e padronanza delle regole (tecniche e principalmente giuridiche) che sottendono all'utilizzo di Internet e, nella fattispecie, del web sommerso.
Grazie al tam tam multimediale che domina il web sono consci che è nella darknet che possono trovare tutto ciò che desiderano, e sanno che qui non corrono il rischio di venire tracciati ed individuati, anche nel caso in cui decidano di compiere azioni illegali.
Per entrare nel web sommerso non sono quindi utilizzabili i comuni motori di ricerca, ma esistono liste di link raggiungibili tramite alcuni siti, nei quali sono presenti un gran numero di collegamenti, ciascuno dei quali, usualmente, inalvea a contenuti allocati su un PC della darknet.
Ciò significa, ovviamente, che se un computer si disconnette, i contenuti presenti su di esso non risulteranno più accessibili in rete.
I collegamenti all'interno della rete sono comunque lenti, ciò è dovuto al fatto che per tutelare l'anonimato degli utenti, i pacchetti di dati non vengono inviati direttamente, ma vengono cifrati e veicolati attraverso rimbalzi tra vari computer.
Nella darknet, l'utente si troverà di fronte ad un web diverso, graficamente scarno, privo di layout grafici attraenti e di colorati banner pubblicitari, la sensazione è quella di trovarsi nel mezzo di un incredibile ed onirico mercato gremito di bancarelle sulle quali è possibile trovare di tutto,
Nei bassifondi del web nulla è proibito, la darknet è stata concepita per essere libera e pirata, un bazar all'interno del quale possono muoversi indisturbati ed aprire vetrine, multimediali mercanti provenienti da ogni parte del mondo, senza scrupoli e pronti a negoziare su tutto.
La valuta utilizzata nel deep web è il bitcoin, una moneta virtuale inventata da un programmatore giapponese, del valore unitario di circa 3,8 euro, strutturata su un sistema di crittografia che rende anonime le transazioni.
Ma, mentre alcuni esperti sostengono che chi fa le indagini potrebbe risalire a chi ha comprato e venduto nel deep web tenuto conto che tutti gli spostamenti di detta moneta sono tracciati da un server, i siti del deep web sostengono che ogni volta che i propri clienti definiscono un affare, i server inviano così tante operazioni fittizie simultanee che risalire ai veri responsabili è virtualmente irrealizzabile.
È però doveroso sottolineare che il deep web non è solo crimine e criminalità, ma una parte del web sommerso ha conservato l'originaria finalità che ne ha determinato la nascita, restando quello spazio virtuale all'interno del quale gli attivisti possono comunicare senza essere intercettati, un centro di ritrovo virtuale di militanti politici e religiosi, ma anche la rete utilizzata dai Governi di mezzo mondo per monitorare le reti terroristiche e le aree in fermento del pianeta.
Da un punto di vista giuridico, utilizzare strumenti di anonimizzazione come proxy o TOR non costituisce reato, così come non rappresenta di per sé una violazione dell'ordinamento giuridico entrare nel deep web; va sottolineato però che poiché i dati cifrati delle connessioni dei vari utenti vengono trasferiti da PC a PC in modo casuale, potrebbe accadere che materiale illegale si trovi a transitare su un determinato computer ad

insaputa del proprietario della macchina, ed a quel punto il reato potrebbe già essersi configurato.
Allo stato non esistono precedenti giurisprudenziali in merito.
Sotto l'aspetto tecnico, l'accesso alla darknet è fortemente sconsigliato principalmente per i pericoli di infezione da malware e di esposizione ad attacchi informatici cui vengono sottoposti i computer dei web surfer nel momento in cui accedono nell'Internet nascosto.
Va tenuto in debito conto, infine, che anche acquistando prodotti legali dai venditori del deep web, nel caso in cui l'utente venga raggirato, non riceva quanto pagato ovvero riceva prodotti non conformi a quanto desiderato, per il compratore sarà praticamente inutile inoltrare querela presso gli Uffici competenti in quanto il rivenditore non sarà in alcun modo individuabile.

Il Coordinatore Nazionale
Raffaele Pinto
392.8836544