ItaliaOggi
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO

diffusione:9304
tiratura:22827

IL PUNTO DI MAURO MASI*

Il lato oscuro e inquietante del web

Allo stato non è dato sapere con certezza se gli attacchi hacker in Italia e in Europa di questi giorni siano degli episodi di guerra ibrida o siano «semplice» cybercriminalità. Quello che invece è certo è che radici e procedure del fenomeno siano da ricercare nel lato «oscuro» del web, quello che nasconde il peggio della rete. Secondo il guru e pioniere del web **Jaron Lanier**, quello che vediamo della rete è solo una frazione ridottissima del traffico online. Infatti l'internet nascosto (deep web), e cioè la porzione che non viene indicizzata dai nostri motori di ricerca, è ormai nettamente in prevalenza nel web effettivo; e all'interno del deep web cresce il dark web, il lato oscuro e inquietante della rete. Nel 2015 nel libro che ho pubblicato per Class Editori (*Internet ci rende più stupidi?*) scrivevo: «La nascita e lo sviluppo dirompente dei social network, così come la fenomenologia del Big Data, hanno reso esplicito quello che fin dagli inizi era implicito nella tecnologia della rete e cioè che su Internet non esiste nessuna privacy. Ma la realtà supera di gran lunga non solo la fantasia ma anche la teoria. Cresce un lato oscuro della rete fatto di violenza, pedofilia, terrorismo, vendita di droga e altre nefandezze che rischia di divorarsi il lato luminoso della rete, quello che ha fatto diventare il web il motore del cambiamento e il faro della modernità». E c'è un pre-requisito essenziale di cui si nutre il lato oscuro: l'anonimato. I sistemi come Tor (The Onion Router) che permettono il sostanziale anonimato del traffico di rete sono ormai divenuti accessibili a chiunque e se in realtà problematiche e particolari possono aiutare a proteggere il dissenso politico e la tutela dei diritti umani (come è effettivamente accaduto ad esempio in Cina o nella Primavera araba e che potrebbe accadere ora in Russia o in Afghanistan), nei Paesi dell'Occidente industrializzato non si vede che senso abbiano. Il funzionamento di Tor si basa su tecniche di triangolazione informatica per cui i dati di qualsiasi comunicazione non transitano come avviene normalmente direttamente dal cliente al server; i server di Tor agiscono da router, costruendo un circuito virtuale crittografato a strati. I siti web creati per Tor hanno un'estensione di dominio specifica chiamata «onion». Essi sono ospitati sul computer del loro creatore e raggiungibili solo navigando attraverso la piattaforma Tor. Ma Tor non è l'unico esempio del genere, esistono e sono ancor più facili da trovare in rete i sistemi Vnp (Virtual private network, rete privata virtuale) che, di fatto, creano una rete privata criptata in una rete pubblica. Vnp è più veloce di Tor ma molto più costoso da mantenere e meno efficace in tema di anonimato assoluto, ma il punto è che è facilissimo da ottenere e installare. Questi sistemi sono il prerequisito essenziale su cui vive il dark web con tutto il suo carico di crimini commessi ogni giorno in ogni parte del mondo. Ora più che mai, è necessario che tutti gli interessati si impegnino perché siano messi rapidamente al bando (o, quantomeno, regolamentati).



Mauro Masi

delegato italiano alla Proprietà intellettuale
Contatti: mauro.masi@bancafucino.it

© Riproduzione riservata

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

