

Esplode nel dark web il traffico illegale di vaccini anti-Covid-19

di Germana Tappero Merlo

Era stato previsto e puntuale è accaduto. Già dal dicembre scorso, l'FBI¹ aveva annunciato il rischio di frodi *on line* legate alle campagne vaccinali da Covid-19. Ed è proprio di alcune settimane fa l'operazione condotta dall'Interpol su un network intercontinentale di traffico di falsi vaccini fra la Cina e il Sud Africa², con centinaia di persone arrestate, per 2400 vaccini falsi e altro materiale medico contraffatto. Cifre importanti ma limitate rispetto a quanto sta emergendo come business criminale, dai numeri decisamente più rilevanti.

Da una recente indagine della società di sicurezza informatica Check Point Software, divulgata in questi giorni dall'emittente americana CNN³, è emerso, infatti, che nel dark web le vendite di vaccini anti-Covid, passaporti vaccinali e addirittura le offerte 3x2 di test di negatività falsi, stanno facendo fare grossi affari a tutto quel mondo di criminali che, in quella parte nascosta di internet, da anni si arricchisce e lucra su ogni tipo di attività e vendite illegali.

Così si possono acquistare vaccini AstraZeneca, Johnson&Johnson dai 750 ai 1000\$ e, se si vuole risparmiare, il russo Sputnik o il cinese SinoPharm a 500-600\$. La stessa società di sicurezza non ha saputo stabilire se si tratta di quelli autentici o dei falsi. Se per quelli veri, infatti, è d'obbligo indagare come i vaccini possano sfuggire e uscire dalle catene ufficiali di smercio senza la criminale compiacenza di chi le produce, allo stesso tempo si può ipotizzare l'esistenza di falle nel sistema di chi li acquista, soprattutto se enti governativi; non meraviglierebbe, invece, se fossero contraffatti, data l'allerta che vige ormai

¹ <https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines>

² <https://www.interpol.int/en/News-and-Events/News/2021/Fake-COVID-vaccine-distribution-network-dismantled-after-INTERPOL-alert>

³ <https://edition.cnn.com/2021/03/23/tech/covid-vaccines-dark-web/index.html>

da anni sulla vendita di falsi medicinali proprio on line, anche nell'internet 'in chiaro', quello più accessibile. Un affare che conta ormai cifre da capogiro (decine di miliardi di dollari) e che si confonde spesso con il mercato delle droghe sintetiche e che fa vittime, moltissime vittime, soprattutto nel Sud del mondo, come l'Africa più povera e malata⁴.

Ma il vero affare è esploso globalmente con la Covid-19: negli ultimi 8 mesi, le registrazioni di domini legati ai vaccini sono aumentate del 300%, e un oltre 29% quello del totale di siti web ritenuti pericolosi, ossia in grado di sottrarre informazioni all'acquirente, dal furto delle credenziali personali alle frodi dalle carte di credito e, appunto, contraffazioni di ogni genere, speculando magistralmente sulle ansie da pandemia di milioni di soggetti. Sono invece autenticamente false le certificazioni, tutte rigorosamente ben riprodotte, che soddisfano la pressante richiesta da parte di soggetti che debbono muoversi nell'immediato da un Paese all'altro per ogni tipo di esigenze personali e non possono attendere i ritardi operativi degli enti nazionali preposti. I passaporti vaccinali, con tanto di nominativo del medico e data di vaccinazione - quelli statunitensi addirittura con il logo del CDC, ossia dei Centri di controllo e prevenzione delle malattie - si aggirano sui 200\$, mentre i falsi test di negatività costano in media 150\$.

Un servizio aperto 24h, che è anche il tempo di consegna massimo una volta inviati dati anagrafici e denaro. Quest'ultimo, poi, meglio se in criptovaluta, tipo Bitcoin, per evitare il tracciamento del pagamento. Da quell'indagine è emerso, inoltre, che da gennaio 2021 gli annunci di vendite di questo tipo nel dark web sono praticamente triplicati e i trafficanti, si ipotizza, siano per lo più statunitensi, spagnoli, tedeschi, francesi e russi. A questi criminali si sta indirizzando un numero crescente di soggetti disoccupati che si offrono come supporto, come money mule, ossia mettendo a disposizione i propri conti correnti come ponte per il passaggio del denaro dall'acquirente al criminale, appunto, da cui la "pulitura" del contante.

Nulla di nuovo, insomma, nel dark web, in quella parte di internet che si accede solo con programmi un po' più complessi, ma poi nemmeno tanto, soprattutto per le nuove generazioni di nativi digitali. Tuttavia, proprio a seguito di questi allarmi da parte di polizie nazionali, FBI, Interpol ed Europol, ed in accordo con costoro, società di cybersecurity stanno utilizzando propri infiltrati nel dark web

⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7197578/>

per contrastare il fenomeno, come avviene per altre attività illecite, dalla pedopornografia, ai traffici di armi e droghe, sino al terrorismo. Un rincorrere, quindi, nell'internet più profondo e nascosto, i responsabili di queste azioni, in attesa che vengano prese misure anche solo per evitare la falsificazione dei passaporti vaccinali, tra cui, fra quelle suggerite proprio dalla Check Point Software, l'uso della crittografia a protezione dei dati e di codici QR con firma digitale, mentre la verifica dell'autenticità potrebbe essere effettuata tramite un repository di informazioni - in pratica un archivio/deposito digitale - centralizzato ma accessibile dalle autorità sanitarie e di polizia di tutti i Paesi.

Ottimi suggerimenti da parte delle società di sicurezza informatica, abituate alla velocità operativa, di decisione e di contrasto. Tuttavia, come per altri fenomeni pericolosi e destabilizzanti globalmente, l'intralcio alla loro applicazione è dato dalla difficoltà di agire compattamente fra i vari Paesi: sono necessari, infatti, reale consapevolezza del problema, dialogo e soprattutto concreta volontà politica per agire efficacemente di concerto, non ultima la condivisione di informazioni circa attività criminali che si stanno ampliando a dismisura, mettendo ulteriormente a rischio la salute pubblica già fortemente compromessa dalla pandemia da Covid-19.