DOPPIOZERO

Falsità in rete

Oliviero Ponte Di Pino 22 Marzo 2024

Dati avvelenati di Giovanni Ziccardi (Raffaello Cortina, 340 pagine 16 €) mette ansia dalla prima all'ultima riga. Ci mette in guarda, come recita il sottotitolo, contro “Truffe, virus informativi e falso online”, con qualche anticipazione sul *trending topic* del momento, l'Intelligenza Artificiale Generativa e i suoi rischi.

Questo viaggio nel lato oscuro della rete è pieno di dati allarmanti. L'aumento degli attacchi informatici con la pandemia, in particolare con l'esplosione del *revenge porn* (p. 29). Il dilagare delle truffe romantiche (p. 139). L'accanimento contro categorie vulnerabili come i minori e gli anziani (nell'ultima parte del volume). I dieci milioni di chiamate false in un anno della piattaforma iSpoof (p. 52-53). In Olanda 15% dei cittadini con più di 15 anni ha dichiarato di essere stato vittima di una o più forme di criminalità online (anche se solo il 20% delle vittime ha denunciato il reato alla polizia) e il 20 per cento degli adolescenti ha dichiarato di aver subito minacce online, bullismo, *stalking* o *revenge porn* (p. 60). Nel 2021 è stata pubblicato un file di oltre 100GB, RockYou2021, con oltre 8,4 miliardi di password rubate (p. 248). Per quanto riguarda i minori, secondo un'indagine della Rutgers University, molte ragazze e ragazzi hanno subito almeno una volta furti di identità (il 20% dei Millennials e il 18% della GenZ) e perdite di denaro a causa di fishing (27% dei Millennials e 34% della GenZ) (p. 62). E l'Italia? Basta leggere il “Resoconto attività 2022 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica”.

In Inghilterra, la National Library è stata messa in ginocchio il 31 ottobre 2023 da un attacco hacker, si è rifiutata di pagare il riscatto richiesto e il ritorno alla normalità sta richiedendo mesi di lavoro e diversi milioni di sterline.

Conseguenze drammatiche hanno gli attacchi ai siti delle strutture sanitarie, assai vulnerabili anche per l'elevato numero di interazioni con l'esterno e la delicatezza dei dati, come spiega lo “Health Threat Landscape” stilato dalla Comunità Europea (scaricabile qui). Anche se qualche scintilla etica pare ancora illuminare il settore: quando un gruppo di hacker si è reso conto di aver reso inutilizzabili

alcuni macchinari di un ospedale pediatrico canadese, in pochi giorni ha diffuso le proprie sentite scuse e il software per rimediare al danno.

I virus e le truffe sono nati con la rete: il primo virus, Elk Cloner, opera di un quindicenne, risale al 1982 (p. 136), nel 1988 Chernobyl ha infettato un milione di computer (p. 144), nel 2000 I Love You ha causato 10 miliardi di danni (p. 145), proprio mentre aleggiava l'ombra del Millennium Bug...

La rete ci può fregare in mille modi, insieme antichi (perché basati sull'avidità, sulla malvagità, sulla credulità, sulla sventatezza di noi umani) e moderni. Si moltiplicano i neologismi, o le vecchie parole riadattate a nuovi usi. Gli *hacker* hanno ormai mille sottospecie, come gli *sneakers* (p. 11) che s'intrufolano in sistemi locali, i *phone phreaker* (o *freakers*), che violano i sistemi telefonici (p. 12). Usano *virus*, *worms*, *trojans*, *ransomware*, *spyware*, *adware*, *keyloggers*, *rootkits* o *botnet* (p. 56), *salami slicing doxing* (p. 56). E poi il *phishing*: qualche anno fa una ridente cittadina rumena, Ramnicu Valcea, venne ribattezzata “la Silicon Valley del furto su internet” perché vi operavano numerosi maghi delle truffe online (p. 174).

Non disponiamo tutti delle competenze necessarie per mettere in atto le complesse strategie necessarie a fregare il prossimo, a estorcergli denaro (ovviamente in bitcoin, anomimi e più facili da far scomparire e ricomparire) per poi incassarlo e farla franca. Chi è interessato può rivolgersi ai servigi di *money mules*, prestanome e *crypto-mixers* (p. 45), *exchanger* e *wallet provider* (p. 47), senza dimenticare *the man in the middle* che s'inserisce nella comunicazione tra due soggetti per intercettare e modificare i dati (p. 57). Per passare al lato oscuro, è opportuno memorizzare il decalogo messo a punto dal re delle truffe Victor Lusting (p. 187-188). Dopo di che, basta ricorrere all'outsourcing: lo *Initial Access Broker* crea un contatto con le apposite reti criminali. Il *crime-as-a-service* mette in rete gli affiliati specializzati che si dividono compiti e ruoli (p. 25).

Ai criminali digitali si stanno aprendo nuovi terreni di conquista. Grazie allo IoT (Internet of Things) sempre più oggetti, dagli elettrodomestici ai veicoli di tutti i tipi, dagli apparati bioingegneristici ai semafori, sono dotati ormai di microcomputer controllati in remoto di cui è possibile prendere il controllo, come insegna il film *Die Hard* (pp. 105-106).

Ziccardi si chiede chi vuole attentare alla nostra sicurezza informatica. Risale ai principali moventi (spionaggio, profitto e ideologia), senza dimenticare l'errore, che diffonde password per sbadataggine e lascia distrattamente aperto l'accesso ai dati sensibili. Individua le quattro principali categorie di cybercriminali: quelli in

proprio, quelli a pagamento, gli Stati e gli attivisti (p. 121). Si moltiplicano sulla stampa internazionale le notizie sugli *State sponsored attacks* (p. 41), nel quadro delle crescenti tensioni internazionali (per non parlare del recente allarme sul sabotaggio dei cavi sottomarini, dove passa buona parte dei dati diffusi in rete). A questi cybercriminali va aggiunta una quinta categoria, quella assai diffusa degli “attori interni”, per esempio il dipendente o l'ex dipendente che vuole vendicarsi del suo datore di lavoro: vedi il caso dell'australiano Vitek Boden, che ha hackerato un sistema di dighe e sversato 800.000 litri di acque reflue non trattate nei fiumi, nei parchi e in aree residenziali. A tutto questo va aggiunto che le vittime denunciano molto di rado il danno: i singoli cittadini per vergogna, le grandi organizzazioni perché lede la loro reputazione e rischia di diffondere informazioni delicate.



Naturalmente il libro è prodigo di consigli più che sensati per difenderci dalle varie minacce e cita doverosamente anche il GDPR della Comunità Europea (p. 220). Ma di fatto chi è costretto a servirsi in maniera sempre più pervasiva di servizi digitali, pubblici e privati, si trova pressoché impotente. Non basta allungare da 8 a 16 bit per le password sempre più numerose che ci assediano: i nostri dati vengono consegnati e custoditi da altri soggetti, pubblici o privati) dei quali siamo costretti a fidarci (firmando contratti lunghissimi, sostanzialmente illeggibili e non negoziabili) e di cui non è bene fidarsi, evidentemente, se sono così vulnerabili da attacchi esterni e defezioni interne.

Ziccardi mette giustamente in guardia contro i siti truffaldini, e cita le sei tipologie con cui la EDPB (il Comitato Europeo per la protezione dei dati) ne identifica la progettazione ingannevole (p. 189). Ma le pagine dei siti social e di molte aziende sono improntate a principi simili, e infatti “risucchiano” e “ingaggiano” gli utenti generando effetti perversi. Le ricerche sugli impatti nefasti dei social sulle giovani generazioni sono ormai purtroppo molto numerose. Non è solo un problema di cybercriminalità, come ci hanno insegnato i casi Snowden e Cambridge Analytica. I primi a violare illegalmente la privacy dei cittadini sono i governi. Quelli autoritari (Cina, Russia, Iran), ma anche quelli “democratici”.

Curiosamente non si accenna alla truffa semilegale (o con regolamenti scarsi e/o poco applicati) del *product placement* degli influencer (con l'indotto dell'evasione fiscale) e della finta beneficenza dei vip, che trova nella rete un fertile terreno. Si parla di *data poisoning*, ovvero di come inquinare le banche dati dei “nemici” (p. 101), ma ormai sappiamo che le banche dati e gli algoritmi presenti in rete sono già *biased*, ovvero portano con sé molti pregiudizi impliciti, in particolare su genere, etnia, classi sociali eccetera. Puntare il dito contro i “criminali” (che in alcuni casi sono attivisti o *whistleblowers*, che rischiano il carcere o peggio) rischia di mettere in secondo piano i rischi strutturali della rete, che non è certo un paradiso terrestre in cui si sono infiltrati alcuni esseri furbi e malvagi.

A lenire l'angoscia, nel panorama delineato da *Dati avvelenati* c'è un aspetto divertente. Perché molte di queste cose le abbiamo già viste al cinema, come racconta Ziccardi nella sua ricca filmografia. Sono ormai decine le pellicole di fiction e i documentari che hanno esplorato (e spesso anticipato) il mondo ibrido e pericoloso in cui siamo immersi, a volte con autentici capolavori.

Non è solo un problema di legalità, di buoni e cattivi. Per fare *phishing*, è necessario fingere di essere un altro. Il furto dei dati personali ci toglie l'identità, lasciandoci nudi e indifesi. L'esproprio della pagina personale sui social strappa via la maschera che ci siamo costruiti con pazienza, post dopo post, storia dopo storia. I data point collezionati su di noi dai *cookies* presenti ormai in ogni sito, setacciando le pagine web dove appaiono il nostro nome, la nostra immagine, la nostra voce, seguendo la geolocalizzazione del cellulare e le espressioni facciali intercettate dalle telecamere di sorveglianza, costruiscono un'identità sulla quale l'interessato non ha alcun controllo. Monetizzando questi dati, espropriandoci delle nostre creazioni e della nostra rete di relazioni, i giganti del web estraggono valore. Tutto legale, naturalmente, perché quello che ci stanno offrendo è una serie di servizi che rendono più facile la nostra vita quotidiana con mille imperdibili consigli per gli acquisti (e censurando quello che potrebbe inibire il

consumo).

Tutto questo sommovimento riguarda la nostra identità e la nostra immagine, il diritto alla privacy, le relazioni interpersonali, il rapporto con la realtà. Ziccardi spiega che le vittime delle truffe online vivono spesso una “bancarotta emotiva”. La rete, per come si è configurata, ci sta espropriando di una parte di noi, anche se ci dà molto in cambio e non possiamo più farne a meno. Per questo le storie ai limiti della fantascienza che raccontano le nostre vulnerabilità digitali, quei documentari che paiono distopie, ci affascinano così tanto.

Se continuiamo a tenere vivo questo spazio è grazie a te. Anche un solo euro per noi significa molto.
Torna presto a leggerci e SOSTIENI DOPPIOZERO



DATI AVVELENATI

Giovanni Ziccardi

TRUFFE, VIRUS INFORMATICI E FALSO ONLINE

Raffaello Cortina Editore