Il Sole 24 ORE

PIRATERIA INFORMATICA

Finanza e cyberattacchi: come entrano in banca e muovono i mercati

—di **Stefano Elli** | 28 novembre 2018

Selce, ascia, balestra, archibugio, revolver, mitragliatrice, tank, missile, byte. Dieci tappe della corsa agli armamenti. L'ultima byte, è la più subdola, in apparenza meno cruenta e sanguinaria. Può mettere in ginocchio il "nemico" colpendo le sue infrastrutture "critiche", sanità, finanza,trasporti, energia. Può manipolare il consenso e i flussi elettorali e, dunque, le decisi politiche. Inserirsi nei sistemi d'arma. Può violare sistemi contenenti informazioni delicatissime come, per esempio, le banc dati della posta elettronica certificata (le Pec) un canale, per fare un solo esempio, su cui a tendere "viaggeranno" dati e atti sensibili, come ordinanze di custodia cautelare e le informative di Polizia giudiziaria ai magistrati. Senza far menzione della recente introduzione della fatturazione elettronica.

Nessuno può dirsi al sicuro

Dal 2012 al 2017 si sono registrati 12 attacchi ai danni delle Banche Centrali. Dalla Federal Reserve di Cleveland a quella di Ne York, dalla Banca Centrale russa alla stessa Banca centrale europea. Nemmeno Banca d'Italia si è salvata: nel 2017 si è registr la violazione della posta elettronica di due ex dirigenti. Nel 2018 In Inghilterra sette delle più grandi banche presenti in inghilterra, Banco Santander, Royal bank of Scotland, Tesco Bank, Hsbc, Lloyds, Clydesdale and Yorkshire Banking group e Barclays, secondo il Financial Times, sarebbero state vittime di intrusioni che le hanno costrette a ridurre drasticamente il numero di operazioni se non a interrompere completamente interi servizi. Il condizionale si deve alla naturale riluttanza del banche in questione ad ammettere pubblicamente le proprie vulnerabilità. Un nuovo tipo di rischio: cybereputazionale. Chi fiderebbe di una banca facilmente «violabile»?

Robocop in movimento

Secondo la National Crime Agency, l'agenzia britannica di contrasto al crimine organizzato, alcune di queste intrusioni si so verificate grazie a software del costo di 11 sterline. E quello della relativa facilità nel rifornirsi di software pirata ha portato d recente alla chiusura di Webstresser.org, una delle piattaforme più attive nella distribuzione di prodotti originariamente concepiti per testare la sicurezza dei sistemi e in realtà utilizzati per violarli

Il settore finanziario in particolare sembra essere sotto attacco. Una delle modalità di intrusione informatica più insidiosa è **Ddos (Distributed Denial of Service)** (interruzione distribuita del servizio, in italiano) . «Più che un intrusione il Ddos è una sorta di sovraffollamento indotto artificialmente in un sistema - spiega Roberto De Vita, presidente dell'Osservatorio Eurisp sulla Cybersecurity - che di fatto rallenta il suo funzionamento e la sua operatività sino a bloccarlo completamente». Realisticamente questo potrebbe diventare un fattore critico di insuccesso. «Provate a immaginare che cosa accadrebbe - spi De Vita - se il concorrente sleale di una piattaforma di trading online provocasse periodicamente dei rallentamenti o dei bloc al sistema del proprio competitor. È evidente che l'indotta inefficienza del sistema causata dal Ddos provocherebbe un allontanamento dei clienti a tutto vantaggio dell'operatore scorretto».

Un altro dei sistemi più utilizzati è certamente quello del **«Man in the middle»** , il pirata che si frappone tra cliente e server d router della banca e comunica con il cliente fingendo di essere quest'ultima, magari intercettando dei bonifici. «Molti episod verificano in virtù di una vulnerabilità comportamentale che potrebbe essere evitata adottando accorgimenti specifici, ma va detto che spesso questo non è sufficiente. - E De Vita prosegue -in generale è possibile affermare che nelle comunicazioni tr persone giuridiche (banche o altri enti) e clienti il grado di sicurezza maggiore la si ha quando questa avviene attraverso gli smartphones. Mentre il web offre molti più varchi ai malintenzionati.

Pirati su tweeter

Ma i rischi di una contaminazione sistemica arrivano anche dai social media. In un rapporto sulla pirateria di Accenture Strategy si cita un esempio da manuale di manipolazione dei mercati condotta attraverso Twitter. Nel 2016 in rete è apparso messaggio di qualcuno che asseriva di essere il ministero degli Interni russo Vladimir Kolokoltsev (e non lo era). Nel messag si dava la notizia, rivelatasi poi falsa, dell'assassinio del presidente siriano Bashar al-Assad. La notizia veniva data tra le 10,15 del mattino e le 10,45. Lo stesso giorno i futures sul petrolio salirono da 90,82 a 91,99 dollari al barile al New York mercantile exchange prima che la notizia fosse ufficialmente smentita.

Intelligenza artificiale e algoritmi

Ciò che sino a ieri era classificato nell'opinione comune come fantascienza oggi rappresenta un problema con cui fare i cont L'uso di algoritmi e di tecniche di autoapprendimento delle macchine (learning machine) e di Intelligenza artificiale. «Faccio solo esempio - spiega De Vita - esistono programmi in grado di utilizzare algoritmi che creano il bitrate delle canzoni e del l testo. O nuovi tipi di intelligenza artificiale basate su reti neurali in grado di comporre musica potendo riconoscere il codice improvvisazione (lo stile) di un musicista. Immaginiamo che cosa potrebbe sorgere da un uso distorto se non criminale di ta funzionalità. Per dare una dimensione di quanto valga il mercato dell'intelligenza artificiale cito due dati: quello del McKinse report 2018 e quello di PriceWaterhouseCoopers dello stesso annpo. Per Mc Kinsey l'AI (intelligenza artificiale) contribuirà a mondiale per una quota di 13 trilioni di dollari da qui al 2030 con un valore medio dell'1,2 annuo. Pwc invece stima il fatto ch l'AI aggiungerà al Pil globale qualcosa come 15,7 trilioni».