CYBERSICUREZZA

La guerra non convenzionale nello spazio cibernetico

di Gloria Valdonio

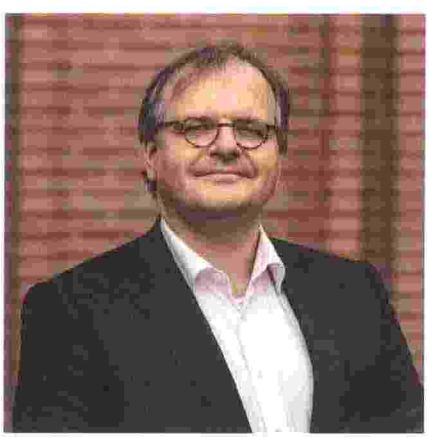
Si stima che nel mondo i costi del cybercrime abbiano toccato l'1,3% del Pil globale e che la cifra dovrebbe aumentare con il conflitto russo-ucraino. L'Italia è in prima fila nella lista dei Paesi vittime di crimini informatici, con attacchi a P.A. e aziende

Qualcuno l'ha definita la "quinta dimensione della conflittualità". Dopo forte spinta verso la digitalizzazione provocata dai lockdown, la guerra russo-ucraina ha fatto letteralmente esplodere il fenomeno del cyber-crime insieme alla consapevolezza dei danni che questo fenomeno comporta per i singoli, le aziende e gli Stati. Ma quali sono le reali dimensioni di questo fenomeno? E quali le implicazioni economiche nei vari Paesi? «Gli attacchi informatici che vediamo ora durante la guerra Russa–Ucraina sono per lo più finalizzati a creare scompiglio in una già complicata situazione, colpendo principalmente il settore energetico», conferma **Patrick Lemmens**, lead portfolio manager fintech di **Robeco**. «Infatti le società più esposte e vulnerabili agli attacchi informatici sono le grandi società in crescita e il settore finanziario, dato che la maggior parte di questi attacchi è realizzata per creare destabilizzazione finanziaria». «La guerra», aggiunge **Stefano Mele**, partner dello studio **Gianni & Origoni** specializzato in cybersecurity e membro del Comitato atlantico italiano, «non ha esasperato il fenomeno della criminalità informatica, che cresce a un ritmo preoccupante, ma ha semplicemente determinato che le organizzazioni criminali si sono concentrate più sulla guerra che non sulle attività criminali di tipo ordinario». E questo perché gli attacchi hacker permettono di svolgere in modalità anonima tutte quelle operazioni di aggressione tipiche di una guerra, senza però dichiararla.

Il profilo dell'hacker

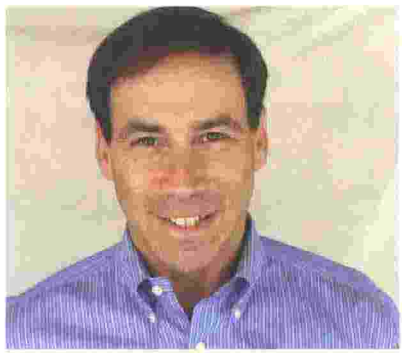
Ma chi sono questi criminali della rete? Molti avranno sentito parlare del famigerato gruppo Conti, un team fluido, ma molto piramidale, di criminali informatici di varie nazionalità, che ha messo a segno alcune delle più redditizie operazioni cyber degli ultimi anni. «Si tratta di un'organizzazione criminale molto attiva, di matrice principalmente russa, ma che conta aderenti di ogni nazionalità, anche ucraini e forse anche italiani», dice Mele. Che aggiunge: «In alcune parti del mondo si può notare una congiuntura tra organizzazioni criminali e Stati, affinché i primi svolgano cibernetiche anche per conto di alcuni governi in cambio della loro impunità criminale». Come spiega Lemmens, gran parte di questi attacchi è compiuta da hacker molto evoluti, residenti in Paesi considerati "poco democratici", che mettono a punto attacchi rapidi e sofisticati. E le grandi banche sono in questa fase costantemente sotto attacco da parte degli operatori del cybercrime. «Possiamo aspettarci che l'hacking di matrice russa aumenti parecchio nei confronti dell'Europa occidentale e degli Stati Uniti, specialmente alle prossime elezioni, in risposta alla guerra in Ucraina e alle sanzioni economiche imposte dai Paesi occidentali», conferma **Anthony Ginsberg**, fondatore di **GinsGlobal Index Funds** e gestore di 3 Etf tematici lanciati da HANetf sul mercato europeo.

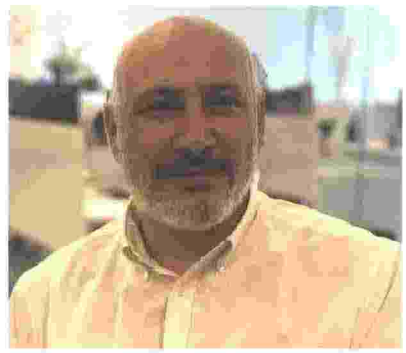
Nella foto Patrick Lemmens, lead portfolio manager fintech di Robeco



Il perimetro

Si stima che i costi legati al cybercrime abbiano toccato l'1,3% del Pil globale. Secondo l'**Internet Crime Report**, invece, le perdite informatiche sono cresciute a 1,8 miliardi di dollari nel 2020, con un aumento del 50% rispetto all'anno precedente, e che oltre 30mila siti web vengono violati ogni giorno, con una media di uno ogni 39 secondi. Il costo dei soli attacchi ransomware nel 2021 è stato stimato a livello globale in 20 miliardi di dollari, il riscatto medio in oltre 300mila dollari e il tempo medio per il ripristino da un attacco ransomware (ovvero il sequestro di dati dal computer per i quali viene chiesto un riscatto) è di 20 giorni. «Sono sufficienti questi numeri per dare un'idea del possibile impatto sulle aziende, anche solo in termini di costi, per mancata





Nelle foto da sinistra, Emanuele Capra, responsabile cyber security e business continuity di Assiteca, Anthony Ginsberg, fondatore di GinsGlobal Index Fund e Diego Marson, cso di Yarix

produttività nel caso in cui un backup dei propri dati sia stato fatto e non intaccato, scegliendo in questo di non scendere a compromessi con i cybercriminali», spiega **Diego Marson**, cso di **Yarix**, divisione digital security di **Var Group**. Il mondo del cybercrime, secondo Marson, ha subìto negli ultimi anni un'evoluzione nella direzione della commodization, verso cioè l'offerta di competenze, servizi e risorse da parte di "fornitori" specializzati nei confronti di quella che è a tutti gli effetti un'economia underground. «La commodization, abbassando la soglia di accesso, ha consentito la messa in atto di attacchi cyber utilizzando modelli di business che prevedono la ripartizione dei proventi delle attività criminose tra il cyber attaccante e il fornitore di servizi e tecnologie a supporto» spiega lo strategist. «È questo il tipico modello utilizzato per attacchi ransomware, e prevede che gli affiliati (cioè gli esecutori materiali dell'attacco, *ndr*) paghino una quota, compresa nel range 10-30%, agli operatori del ransomware».

La situazione italiana

L'Italia è in prima fila nella lista dei Paesi vittime del cybercrime. Come racconta Mele, dai dati più recenti emerge che siamo tra i primi Paese al mondo e in Europa come bersaglio dei crimini informatici legati all'ottenimento di un vantaggio economico, come appunto i ransomware. Ma da cosa nasce questa situazione in Italia? «Come ha recentemente dichiarato il Ministro **Vittorio Colao**, il 95% dei sistemi informatici italiani della PA è vulnerabile. Questa può essere senz'altro una delle ragioni più evidenti», afferma Mele. In altre parole, se un Paese ha un basso livello di difesa, è ovvio che i pirati informatici si dirigano su quel Paese. Ma quali sono i bersagli più sensibili? «Gli attacchi sono diretti prevalentemente alle strutture pubbliche: la pubblica amministrazione è oggetto infatti del 69% degli attacchi ransomware, l'industria privata del 24% e il restante 7% verso privati», spiega Mele. Per prevenire gli attacchi, secondo Mele, è necessario abbandonare l'idea della straordinarietà. «Gli attacchi alle aziende e alla PA in Italia sono quotidiani e non eccezionali. La base di partenza per una difesa efficace è capire che, con migliaia di attacchi al giorno, l'allerta deve essere costante».

Evoluzione

Molti sostengono che il cybercrime sia esploso con la pandemia. E che il lockdown, con la diffusione dello smartworking e la digitalizzazione spinta dei processi e dei servizi pubblici, sia stata la miscela perfetta per il proliferare degli attacchi criminali. «Con il lavoro da remoto cresce il rischio di subire un attacco informatico», conferma Lemmens. «Abbiamo perciò assistito alla crescita della domanda dei servizi di cybersecurity e degli investimenti delle aziende nei sistemi di protezione». "Gli attacchi hacker», aggiunge Ginsberg, «saranno sempre più inclusi nelle nuove strategie belliche e nelle cosiddette "guerre ibride" che si potrebbero giocare in futuro. I governi in Ue e negli Usa stanno aggiornando i loro servizi di sicurezza informatica, portando a un aumento della spesa, ma questi aggiornamenti richiederanno tra i sei e i dodici mesi per essere implementati completamente». Come spiega **Emanuele Capra**, responsabile cyber security e business continuity di **Assiteca** (primo broker assicurativo italiano), all'attività criminale la guerra ha aggiunto la componente distruttiva e il bersaglio sono prevalentemente le aziende produttive italiane. «Abbiamo clienti italiani colpiti da vecchi malware riesumati con la guerra, che cancellano tutti i dati distruggendo il patrimonio aziendale con un colpo di spugna», spiega Capra. Che aggiunge: «Il rischio cibernetico è uno dei rischi più impattanti e la guerra non ha fatto che risvegliare una serie di problemi molto impattanti per l'economia che c'erano già, come gli incidenti informatici nella supply chain nel mondo dei traporti e della logistica». Le contromisure? «Innanzitutto l'aggiornamento dei servizi di sicurezza su Cloud e attività di smart working. Per questo ci aspettiamo un aumento dell'attività di M&A in quest'area, poiché è probabile che sempre più servizi di cloud e cybersecurity vengano offerti come un unico pacchetto per contrastare l'aumento degli attacchi», spiega Ginsburg. Che conclude: «Prevediamo che proprio la spesa del settore Cloud si avvicini al 50% della spesa IT globale entro il 2025, con la cybersecurity come primo beneficiario».

Nella foto Johan Vad der Biest, Lead Manager del Candriam Robotics and Innovative Technologies Fund