# L’identikit del cybercriminale e come proteggersi

A cura di Yves Kramer, Senior Investment Manager di Pictet Asset Management

09.11.2023

- ***Tra il 2021 e il 2025, la spesa annua cumulativa in cybersecurity dovrebbe raggiungere 1,75 mila miliardi di dollari. Al contempo, i costi globali della criminalità informatica dovrebbero salire fino a 10,5 mila miliardi di dollari annui entro il 2025.***
- ***Gli attacchi informatici rappresentano già oggi un problema enorme: ogni 39 secondi un hacker riesce a infiltrarsi in un sistema e ogni giorno vengono rubati circa 3,8 milioni di record tramite violazioni. Non sorprende che, da attese, il settore della sicurezza informatica crescerà nell’ordine del 14% quest’anno, secondo Gartner.***
- ***La sfida per le aziende di sicurezza sarà sviluppare una nuova generazione di strumenti di sicurezza informatica che incorporino tecnologie come l’IA generativa per consentire il riconoscimento dei malware in modo rapido e su vasta scala.***

Il mese di ottobre ha riportato l’attenzione sul tema della cybersicurezza. L’European Cybersecurity Month (ECSM), promosso dall’Agenzia dell'Unione europea per la cybersicurezza (ENISA), ha messo al centro della campagna di sensibilizzazione di ottobre 2023 il fenomeno del social engineering, l’insieme delle tecniche utilizzate dai cybercriminali volte a convincere un obiettivo a rivelare informazioni specifiche o a eseguire azioni per motivi illegittimi. Come scrive l’istituto europeo, l’atteggiamento del cybercriminale è noto: sfrutta leve come l’empatia e la compiacenza per ingraziarsi la propria vittima, facendo leva sull’urgenza della richiesta e la capacità di risolvere problemi (spesso creati dallo stesso criminale) per ottenere informazioni o denaro e far perdere le proprie tracce.
Nel mondo online, spesso senza consapevolezza, le persone condividono dal loro smartphone alcune delle informazioni più importanti della propria sfera personale, sia tramite i social network, che (soprattutto) attraverso applicazioni bancarie, portali sanitari, cassetti fiscali o servizi di messaggistica. Ciò genera una mole enorme di dati personali condivisi, di cui spesso si trascura il livello di sicurezza.

**Assicurare la sicurezza dei dati**
La sicurezza digitale e quella dei dati sono temi estremamente delicati. In un contesto in cui esiste ancora poca consapevolezza, le grandi aziende stanno mobilitando enormi somme di investimenti per assicurare la sicurezza dei propri utenti. Tra il 2021 e il 2025, la spesa annua cumulativa in cybersecurity dovrebbe raggiungere 1,75 mila miliardi di dollari. Al contempo, i costi globali della criminalità informatica dovrebbero salire fino a 10,5 mila miliardi di dollari annui entro il 2025 [1]. La mancata prevenzione, dunque, può costare cara.
A questi dati si aggiunge la portata dell’Intelligenza Artificiale, che avrà un duplice effetto: da un lato l’integrazione di IA permetterà di rendere più efficaci i sistemi di protezione, ottimizzando il tempo impiegato per il rilevamento delle minacce, velocizzando l’offerta di soluzioni e migliorando la protezione dell'identità e del flusso di dati; dall’altro, però, renderà sempre più sofisticati gli attacchi perpetrati, complicherà gli effetti per l’infrastruttura e amplierà il target.
Implementare nuova tecnologia per sfruttare i benefici e proteggersi dagli effetti dell’IA (elemento chiave di performance di mercato da inizio 2023, soprattutto per strategie legate al digitale e alla

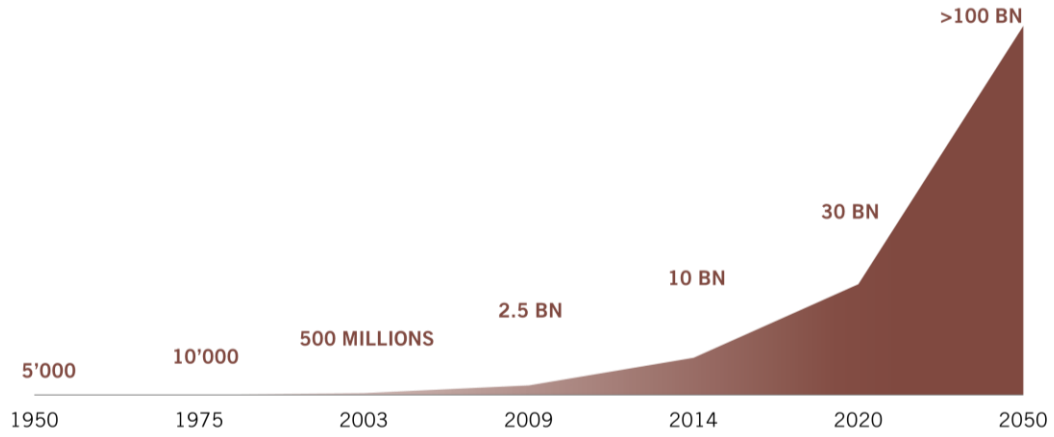
[1] Fonte: Cybersecurity Ventures, Barkly.com, “5 must-know cybersecurity data”

robotica) diverrà fondamentale nei prossimi mesi e anni. Gli attacchi informatici rappresentano già oggi un problema enorme: ogni 39 secondi un hacker riesce a infiltrarsi in un sistema[2] e ogni giorno vengono rubati circa 3,8 milioni di record tramite violazioni[3]. Non sorprende che, da attese, il settore della sicurezza informatica crescerà nell'ordine del 14% quest'anno, secondo Gartner. Tuttavia, data la presenza capillare dell'IA, riteniamo che la crescita possa accelerare ulteriormente in futuro, aprendo una grande opportunità per le società aperte ad accogliere il tema della digitalizzazione. Sempre in base alle stime, quest'anno due terzi delle aziende americane aumenteranno i propri investimenti in sicurezza informatica rispetto al 2022, con il timore principale di perdite finanziarie[4].

## Nuove esigenze di sicurezza

È proprio partendo dalla consapevolezza del tema che si può capire il potenziale che ancora esiste in tale ambito. Nuove tecnologie aprono nuove esigenze di sicurezza: sempre più le città intelligenti utilizzeranno tecnologie dirompenti (l'Internet of Things) per affrontare sfide demografiche, economiche, ambientali, infrastrutturali e sociali e richiederanno investimenti in infrastrutture, mobilità ed edilizia smart.

**Numero di dispositivi connessi**




Fonte: IBM Institute for Business Value, "Device democracy"

La sfida per le aziende di sicurezza sarà sviluppare una nuova generazione di strumenti di sicurezza informatica che incorporino tecnologie come l'IA generativa per consentire il riconoscimento dei malware in modo rapido e su vasta scala. Lo sviluppo tecnologico potrebbe portare alla creazione di nuovi sottosettori di sicurezza informatica, ad esempio, creando un nuovo mercato per il controllo delle informazioni generate dai sistemi di IA.

Più in generale, data la persistente incertezza economica, riteniamo che la priorità di aziende e governi sarà garantire le infrastrutture critiche dei Paesi, proteggere l'integrità dei cittadini e garantire la capacità delle imprese di raggiungere i propri obiettivi. Il conflitto Russia-Ucraina e l'escalation delle tensioni israelo-palestinesi, temi strutturali chiave, ridefiniranno temi quali la sicurezza informatica, il reshoring e la sicurezza delle catene di approvvigionamento. Il cyberspazio si è rivelato la nuova frontiera della guerra: le difficoltà diplomatiche internazionali hanno ulteriormente evidenziato la crescente importanza della sicurezza informatica per proteggersi da attacchi informatici coordinati. A tal proposito, prevediamo che la domanda europea di prodotti di cybersecurity accelererà nel breve e medio termine, per recuperare il ritardo rispetto agli Stati Uniti e all'Asia.



[2] https://ung.edu/continuing-education/news-and-media/cybersecurity.php

[3] https://business.bofa.com/content/dam/flagship/bank-of-america-institute/transformation/cybersecurity-landscape-impact-what-comes-next.pdf

[4] 2023 Gartner CIO and Technology Executive Survey

***Il Gruppo Pictet***

*Fondato a Ginevra nel 1805, il Gruppo Pictet è uno dei principali gestori patrimoniali e del risparmio indipendenti in Europa. Con un patrimonio gestito e amministrato che ammonta a circa 653 miliardi di euro al 30 giugno 2023, il Gruppo è controllato e gestito da otto soci e mantiene gli stessi principi di titolarità e successione in essere fin dalla fondazione. Il Gruppo Pictet, con oltre 5.300 dipendenti, ha il suo quartier generale a Ginevra e altre sedi nei seguenti centri finanziari: Amsterdam, Barcellona, Basilea, Bruxelles, Dubai, Francoforte, Hong Kong, Londra, Losanna, Lussemburgo, Madrid, Milano, Montreal, Monaco di Baviera, Nassau, New York, Osaka, Parigi, Principato di Monaco, Roma, Shanghai, Singapore, Stoccarda, Taipei, Tel Aviv, Tokyo, Torino, Verona e Zurigo. Pictet Asset Management ("Pictet AM") comprende tutte le controllate e le divisioni del Gruppo Pictet che svolgono attività di asset management e gestione fondi istituzionali. Fra i principali clienti si annoverano alcuni dei maggiori fondi pensione, fondi sovrani e istituti finanziari a livello mondiale.*

**Contatti Stampa:**
**BC Communication**
Lucrezia Pisani | Tel. +39 347 6732479 | lucrezia.pisani@bc-communication.it
Carla Parisi | Tel. +39 339 5796751 | carla.parisi@bc-communication.it