È l'allarme lanciato dal Rapporto Clusit: lo scorso anno si sono verificati 2.779 incidenti

Cybercrimine, Italia nel mirino

Gli attacchi gravi crescono del 65% contro il 12% globale

Pagina a cura
DI ROXY TOMASICCHIO

L'Italia è nel mirino degli attacchi informatici, con tecniche sempre più affinate, anche grazie al ricorso all'Intelligenza artificiale. Lo scorso anno la crescita degli attacchi cyber gravi, cioè con un impatto ad ampio raggio, su ogni aspetto della società, della politica, dell'economia e della geopolitica, si è rivelata maggiore rispetto al resto del mondo. Numeri alla mano si tratta del +65% rispetto al 2022, in Italia, contro il +12% a livello mondiale. L'11% degli attacchi sferrati in tutto il mondo, per un totale di 310 incidenti, è stato indirizzato, ed è andato a segno, nel nostro Paese. Nel 2022 il dato era fermo al 7,6%. Oltre la metà degli attacchi (il 56%) ha comportato effetti di gravità critica o elevata. Non solo. Ha visto come vittima l'Italia quasi un attacco su due (47%) di matrice hacktivism (ossia gli attacchi informatici per finalità politiche o sociali, soprattutto dimostrative. Caso tipico sono gli attacchi contro le forze dell'ordine).

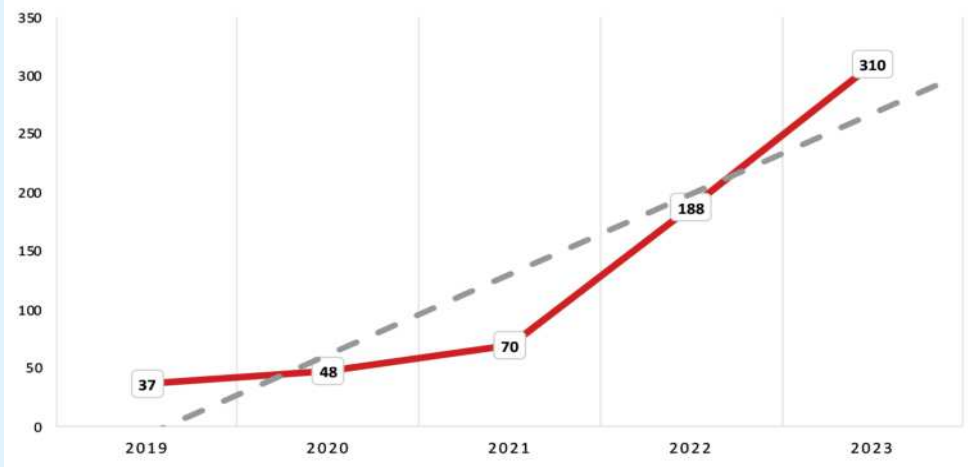
Sono alcuni dei dati raccolti nel Rapporto 2024, di **Clusit**, Associazione italiana per la sicurezza informatica, giunto al dodicesimo anno di pubblicazione, che sarà presentato in apertura del Security Summit, convegno dedicato ai temi della cyber security in programma a Milano dal 19 al 21 marzo prossimi.

L'andamento degli attacchi a livello globale. Non si arresta la curva di crescita degli incidenti gravi, con 2.779 episodi registrati lo scorso anno. Ogni mese è stata rilevata una media di 232 attacchi, con un picco massimo di 270 ad aprile 2023, che rappresenta anche il valore più elevato registrato negli anni. Dal 2018 al 2023 gli attacchi sono cresciuti del 79%, con la media mensile passata da 130 a 232.

In otto casi su dieci, la gravità degli attacchi è elevata o critica. Dati allarmanti, ma che fotografano solo una parte del fenomeno, visto che molte vittime mantengono riservate le informazioni sugli attacchi cyber subìti e visto che in alcune zone del mondo la possibilità di accesso alle informazioni è molto limitata.

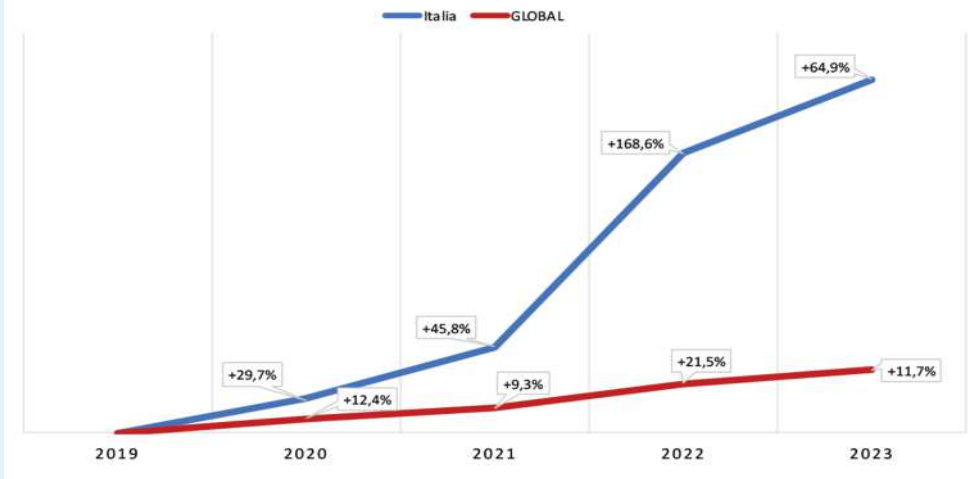
Come anticipato, per quanto riguarda le tecniche, non bisogna abbassare la guardia sull'utilizzo dell'Intelligenza artificiale da parte dei cyber criminali per selezionare i target e scansionarli, con l'obiettivo di trovare falle, per analizzare codici e trovare nuove vulnerabilità e per produrre contenuti per phishing o codice per malware. Si tratta di una tendenza in rapida ascesa, di cui tuttavia i ricercatori di Clusit ritengono sarà possibile osservare gli effetti solo in un prossimo futuro.

Gli attacchi in Italia



Fonte: Rapporto Clusit 2024

La crescita percentuale a confronto



Fonte: Rapporto Clusit 2024

L'analisi degli attacchi in Italia. Tra il 2019 e il 2023, sono stati 653 gli attacchi noti e di particolare gravità messi a segno in Italia; di questi oltre il 47% (310, appunto) sono avvenuti lo scorso anno. Il ritmo di crescita, quindi, è serrato e indica sia la tendenza dei cyber criminali di mirare sul nostro Paese, sia una scarsa capacità, da parte delle imprese, di difendersi, malgrado gli investimenti in sicurezza siano in aumento, come riscontrato dall'osservatorio Cybersecurity e Data Protection del Politecnico di Milano (si veda *ItaliaOggi Sette* del 4 marzo 2024). «Le strategie adottate a oggi, anche a livello normativo a livello sia italiano che europeo, sono state sicuramente utili e importanti per cercare di limitare la crescita del fenomeno. Ma per poter far rallentare il trend e cercare di stabilizzarlo, e possibilmente ridurlo, devono essere concepite e adottate strategie nuove che si fondino sul knowledge sharing, sulla messa a fattor comune degli investimenti», commenta **Gabriele Faggioli**, presidente di Clusit, che aggiunge «Vogliamo mantenere alta l'attenzione anche sulla frammentazione di infrastrutture e servizi che caratterizza la cyber security nel nostro Paese, e che rischiano di produrre una moltiplicazione di sforzi, ciascuno in sé poco efficace, come ampiamente dimostrato dai settori di mercato maggiormente colpiti e anche considerando la spesa complessiva italiana in cybersecurity».

Gli obiettivi nel mondo e in Italia. I ricercatori Clusit, analizzando gli attacchi noti dello scorso anno, indicano una prevalenza di quelli con lo scopo di estorcere denaro (cosiddetto cybercrime), che sono stati oltre 2.316 a livello globale (più dell'83% del totale), in crescita del 13% rispetto al 2022. Un dato, a parere degli autori del Rapporto, che si traduce in un legame stretto tra criminalità "off-line" e criminalità "on-line". Sono quasi triplicati, invece, nel mondo, gli attacchi con matrice di hacktivism, pari all'8,6% del totale (erano il 3% nel 2022), con una variazione percentuale rispetto al totale anno su anno del 184%. In significativa diminuzione, invece, i fenomeni di espionage (6,4%, 11% nel 2022) e information warfare (1,7%, 4% nel 2022).

In Italia, nel 2023 gli attacchi con finalità di cybercrime sono stati pari al 64%; segue un 36% di attacchi con finalità di hacktivism, in netta crescita rispetto al 2022 (6,9%), con una variazione percentuale anno su anno del +761%. Il 47% circa del totale degli attacchi con finalità "hacktivism" a livello mondiale è avvenuto ai danni di organizzazioni italiane, a dimostrare l'attenzione di gruppi di propaganda che hanno l'obiettivo di colpire la reputazione delle organizzazioni. Questa tipologia di eventi, in particolare quelli avvenuti nei primi nove mesi dell'anno, secondo i ricercatori di Clusit, è legata per la maggior parte al conflitto in Ucraina, nei quali gruppi di attivisti agiscono mediante campagne dimostrative rivolte tanto al nostro Paese che alle altre nazioni del blocco filo-ucraino. A ulteriore conferma che siamo in una fase di guerra cibernetica diffusa ci sono gli attacchi con finalità di spionaggio e guerra delle informazioni (espionage e information warfare), aumentati da valori prossimi al 50% nel 2022 a valori intorno al 70% lo scorso anno. Questo andamento, infatti, si può spiegare con riferimento ai conflitti Russo-Ucraino e Israelo-Palestinese.

Chi viene attaccato nel mondo e in Italia. A livello mondiale le principali vittime appartengono ai cosiddetti obiettivi multipli (19%). A seguire il settore della sanità (14%) che ha subito un balzo del 30% e inoltre gli incidenti in questo settore hanno visto un aumento della gravità dell'impatto, critico nel 40% dei casi (era il 20% nel 2022). E ancora: parte consistente degli attacchi è stata rivolta anche al settore governativo e delle pubbliche amministrazioni (12%); al settore finanza e assicurazioni (11%).

Il settore più attaccato in Italia nel 2023 è stato invece quello governativo/ militare, con il 19% degli attacchi (+50% rispetto al 2022); seguìto dal manifatturiero, con il 13% (+17%). Colpito dal 12% degli attacchi, il settore dei trasporti/logistica in Italia, ha visto invece un incremento percentuale anno su anno sul totale degli attacchi del 620%; analogamente, il settore della finanza e delle assicurazioni, verso cui è stato portato a termine il 9% degli attacchi nel 2023, ha visto una variazione percentuale sul totale del +286%.

Le vittime appartenenti alla categoria degli "obiettivi multipli" sono state colpite nel nostro Paese dall'11% degli attacchi, segno di una maggior focalizzazione dei cyber criminali verso settori specifici negli ultimi mesi.

I continenti più colpiti. La distribuzione geografica percentuale delle vittime, secondo i ricercatori di Clusit, riflette la diffusione della digitalizzazione. Sono stati più numerosi, infatti, nel 2023 come nel 2022, gli attacchi alle Americhe, che corrispondono al 44% del totale. Gli attacchi rivolti all'Europa hanno rappresentato il 23% degli attacchi globali, scendendo di un punto percentuale rispetto all'anno precedente ma in crescita sul 2022 del 7,5%. Crescono invece di un punto percentuale rispetto al 2022 gli attacchi in Asia (9% del totale); stabili quelli in Oceania e in Africa, rispettivamente il 2% e l'1% del totale.