VARGROUP

Y-REPORT 2026 - IX EDIZIONE

Cybersecurity: mezzo milione di eventi di sicurezza, ransomware in crescita del 51% e pressioni geopolitiche il volto della minaccia digitale nel 2025

L'Italia abbandona la top 5 dei Paesi più colpiti dai ransomware; Lombardia (36%), Emilia-Romagna (13%) e Lazio (11,63%) le regioni più colpite

Sumud Flotilla e crisi geopolitiche alimentano le campagne hacktiviste: due picchi di attacchi in Italia tra giugno-luglio (27,7%) e settembre-ottobre (23,5%) nel 2025

Milano, 7 maggio 2026 – **Yarix**, centro di competenza per la cybersecurity dell'azienda **Var Group**, presenta la nuova edizione del suo report annuale sugli eventi di sicurezza osservati nel corso del 2025. Il nuovo rapporto fotografa un anno di forte accelerazione del rischio cyber tra ransomware, compromissione delle identità e pressione geopolitica

Nel 2025, il Security Operations Center di Yarix ha esaminato **oltre 522 mila eventi di sicurezza**. Di questi, **più di 158 mila si sono evoluti in incidenti veri e propri**, con un incremento medio mensile **dell'8%** rispetto al 2024. **Particolarmente significativo è l'aumento degli eventi più gravi, con +62% su base annua**, confermando una maggiore capacità degli attaccanti di colpire in modo mirato e impattante.

Dall'analisi settoriale emerge una chiara concentrazione degli attacchi verso **organizzazioni produttive e tecnologiche ad alta criticità operativa:** i settori maggiormente colpiti sono il Manufacturing (**17,9%**) e l'IT (**8,3%**). Nel primo caso, pesano sistemi produttivi obsoleti le cui risorse non sono centralizzate in un unico punto, ma disperse su più nodi, che aumentano la superficie di esposizione. Nel settore IT, invece, incidono la quantità e la sensibilità dei dati trattati e l'alto numero di servizi accessibili dall'esterno.

Malware e accessi iniziali: attacchi più silenziosi e persistenti

La crescita complessiva è indicativa di una trasformazione più ampia del panorama delle minacce. Il 2025 evidenzia infatti un'evoluzione verso **modelli di attacco più distribuiti, automatizzati e adattivi**, in cui gli attori malevoli sfruttano in modo sempre più efficace la combinazione di vulnerabilità note, credenziali compromesse e superfici esposte.

Questo si traduce in una **riduzione del tempo tra accesso iniziale e potenziale impatto**, aumentando la necessità di individuare tempestivamente segnali anche deboli ma significativi.

Uno dei principali driver degli attacchi è rappresentato dalle **tecniche di Initial Access**: l'abuso di credenziali valide, l'esposizione di servizi accessibili da Internet e l'evoluzione delle campagne di phishing, sempre più sofisticate e difficili da distinguere da comunicazioni legittime, delineano un modello di attacco in cui la prima fase della kill chain assume un ruolo determinante.

L'analisi evidenzia inoltre come gli eventi osservati siano sempre meno isolati e sempre più parte di **catene di attacco articolate**, in cui più tecniche vengono combinate per aggirare i controlli di sicurezza.

Ransomware: crescita globale e Italia fuori dalla Top 5

Nel 2025, **a livello globale**, Yarix ha monitorato **oltre 7.100 attacchi ransomware rivendicati pubblicamente, con un aumento del 51% rispetto al 2024** e un numero crescente di gruppi attivi. La minaccia appare sempre più frammentata: accanto a **pochi attori dominanti**, emergono decine di nuovi gruppi con impatto più limitato (+35% gruppi attivi registrati).
In una classifica composta da 124 gruppi ransomware attivi nel 2025, la Top 10 concentra da sola circa il 56% degli attacchi complessivi.

Sul piano geografico, **gli Stati Uniti restano il Paese più colpito (52%)**, seguiti a distanza da Canada (6%) e dai Paesi dell'Europa occidentale (Germania, Regno Unito, Francia, insieme 10%). **L'Italia, dopo anni nella Top 5, scende al sesto posto.**
Le vittime ransomware a livello nazionale sono prevalentemente piccole (67%, +10% rispetto alla media globale) e medie imprese (18%). A livello territoriale, **Lombardia (36%), Emilia-Romagna (13%), Lazio (10%), Veneto (10%) e Piemonte (8%)** risultano le regioni più colpite, riflettendo la concentrazione del tessuto produttivo e industriale.

Il totale degli attacchi attribuiti ai paesi presenti nella Top 10 rappresenta il 77% degli eventi complessivi registrati nel 2025.

Hacktivism e geopolitica: l'Italia nel mirino delle campagne dimostrative

Accanto alla criminalità cyber, il 2025 ha visto una forte attività di hacktivismo contro obiettivi italiani, con attacchi DDoS e defacement utilizzati come strumenti di pressione e propaganda. Le campagne si sono sviluppate "a ondate", con picchi in corrispondenza di eventi geopolitici ad alta visibilità, dal conflitto in Ucraina al conflitto tra Israele e Hamas.

- Il primo picco, il più marcato, si colloca tra i mesi di giugno e luglio, periodo in cui si concentra complessivamente oltre il 27% degli attacchi osservati. Questa fase coincide con una forte attenzione mediatica sul ruolo dell'Italia in ambito NATO e nel sostegno all'Ucraina. In particolare, l'avvicinamento al vertice NATO dell'Aja di fine giugno (dove **gli alleati si sono impegnati a investire in difesa e sicurezza fino al 5% del PIL annuo entro il 2035**) e le discussioni sul rafforzamento delle politiche di difesa europea hanno fornito un contesto facilmente sfruttabile dai collettivi hacktivisti filorussi, che hanno utilizzato le rivendicazioni cyber come strumento di pressione comunicativa.

- Nello stesso intervallo temporale si inserisce anche la Conferenza sulla Ripresa dell'Ucraina (URC2025), ospitata a Roma il 10 e 11 luglio. L'evento, ad alta visibilità internazionale e simbolicamente legato alla ricostruzione di Kiev, è stato più volte richiamato nelle narrative utilizzate dai gruppi hacktivisti per giustificare azioni dimostrative contro obiettivi italiani, rafforzando il legame tra cyberattacchi e posizionamento geopolitico.

- Un secondo picco significativo si registra tra settembre e ottobre, con circa il 23% delle campagne concentrate in questa finestra temporale. In questa fase, l'attività hacktivista appare fortemente influenzata da ricorrenze simboliche e da dinamiche legate al conflitto tra Israele e Hamas. In particolare, l'anniversario del 7 ottobre si conferma un potente catalizzatore per campagne coordinate, promosse da collettivi pro-palestinesi e pro-arabi, che estendono le proprie azioni anche verso Paesi percepiti come sostenitori di Israele, tra cui l'Italia. Tra i bersagli colpiti figurano anche istituzioni ad alto valore simbolico. Nel periodo immediatamente precedente al 7 ottobre 2025 alcune università italiane, tra cui **La Sapienza di Roma** e **l'Alma Mater Studiorum di Bologna** hanno subito attacchi DDoS avvenute in concomitanza con proteste studentesche pro-Palestina già in corso nelle stesse città, suggerendo un chiaro intento di amplificazione reciproca tra mobilitazione fisica e attivismo digitale.

- All'interno di questo contesto trovano spazio anche riferimenti ricorrenti alla **Sumud Flotilla**, citata nelle rivendicazioni come simbolo di resistenza e come elemento narrativo utile a rafforzare il messaggio politico delle azioni cyber. Le operazioni vengono spesso accompagnate da hashtag, comunicati e contenuti propagandistici, con l'obiettivo di massimizzare la visibilità online più che di provocare danni tecnici duraturi.

"Il 2025 rappresenta un passaggio di maturità per il contesto cyber: non ci troviamo più soltanto di fronte a una crescita dei numeri, ma a un cambiamento profondo delle modalità con cui la minaccia si manifesta. Gli attacchi sono diventati più veloci, frammentati e capaci di adattarsi rapidamente, sostenuti da un ecosistema criminale ormai strutturato e dall'accesso sempre più diffuso a strumenti avanzati, compresi quelli basati sull'intelligenza artificiale. In questo quadro, il ransomware continua a essere uno degli strumenti principali di pressione economica, mentre la componente geopolitica incide in modo crescente anche sul panorama italiano, rendendo il rischio informatico strettamente legato agli equilibri globali. Per le organizzazioni, il cambiamento più significativo riguarda il ruolo stesso della sicurezza, che evolve da funzione prevalentemente tecnica a fattore strategico. In questo scenario, il vero vantaggio competitivo non sarà tanto evitare l'attacco, quanto essere in grado di governarlo, ridurne l'impatto e trasformarlo in un'opportunità di miglioramento continuo", **ha dichiarato Mirko Gatto, Head of Cybersecurity di Var Group,** commentando la dimensione cyber del conflitto. "*Nei prossimi anni diventerà sempre più evidente il passaggio da una cybersecurity semplicemente "dichiarata" a una cybersecurity "dimostrabile". Normative come la NIS2, insieme all'evoluzione del panorama delle minacce, spingeranno le organizzazioni verso modelli fondati su governance, tracciabilità, controlli costanti e reale capacità di risposta.*»

Metodologia

L'analisi si basa sui dati raccolti ed elaborati da Yarix nel corso del 2025, assunto come periodo di osservazione. Il dataset include informazioni derivanti da un panel qualificato di organizzazioni clienti, rappresentative di diversi settori dell'economia nazionale e internazionale, nonché dati relativi alla gestione di incidenti informatici presso aziende non precedentemente servite, supportate nelle fasi di risposta e ripristino operativo.

Le organizzazioni incluse nel panel presentano, in media, oltre 1.000 dipendenti e un fatturato superiore ai 50 milioni di euro, garantendo una base dati significativa e rappresentativa di realtà enterprise e mid-market.

Tutti i dati sono stati sottoposti a processi di normalizzazione e aggregazione statistica, al fine di assicurare coerenza e affidabilità nelle analisi. Le informazioni sono state inoltre anonimizzate automaticamente, eliminando qualsiasi possibilità di ricondurre i dati alle singole organizzazioni, nel pieno rispetto della riservatezza.

Var Group

Var Group è l'operatore leader nel settore dei servizi e delle soluzioni digitali, con un fatturato di 875,7 milioni di Euro al 30 aprile 2025. Grazie alla professionalità delle oltre 4243 persone, accompagna le imprese nel loro percorso di trasformazione digitale. Ha una presenza territoriale in 16 paesi nel mondo (Italia, Albania, Andorra, Austria, Benelux, Brasile, Francia, Germania, India, Messico, Romania, Spagna, Svizzera, Thailandia, Tunisia e USA) e una profonda conoscenza dei processi aziendali che le permettono di essere vicina agli imprenditori nella definizione di modelli di business evoluti. L'offerta Var Group si arricchisce costantemente grazie alla ricerca continua e alla stretta collaborazione con i più importanti brand tecnologici e digitali, start up e poli universitari, che le consentono di essere al fianco dei maggiori distretti industriali quali Food & Beverage, Pharma, Automotive, Mechanical, Fashion & Luxury, Furniture, GDO & Retail, Finance e PA, esaltandone l'eccellenza. La sinergia e la specializzazione dei suoi centri di competenza permettono alle imprese di sfruttare al meglio i benefici del digitale e di sviluppare progetti in ambito Multimedia & Workspaces, Business Applications, Digital Experience, Industry Solutions, Cyber Security, Data Science, Digital as a Service, Digital Evolution, Industrial Digital Twin e Sustainability Solutions.
Nel novembre 2025 si è riconfermata per il quarto anno consecutivo un Great Place To Work Italia, posizionandosi nella top 10 della "Classifica Best Workplaces™ Italia 2025" con oltre 1000 persone. Var Group aderisce al Global Compact ONU, promuove attivamente il suo impegno in ambito ESG sviluppando numerosi progetti, documentati nel primo bilancio di sostenibilità volontario del 2024.

Fa parte del Gruppo Sesa, operatore di riferimento in Italia nell'offerta di innovazione tecnologica e soluzioni informatiche e digitali per il segmento business con ricavi consolidati per Euro 3,357 Miliardi di ricavi al 30 aprile 2025. Sesa S.p.A. è quotata sul mercato Euronext STAR Milano e persegue una strategia di sviluppo sostenibile a beneficio dei propri Stakeholder basata sulle competenze delle risorse umane e l'attenzione alla responsabilità ambientale e sociale.

Yarix

Yarix è il brand di competenza per la cybersecurity di Var Group e uno dei più riconosciuti, innovativi e autorevoli player italiani nel settore della sicurezza informatica. Da 25 anni fornisce servizi e soluzioni di cyber security e business continuity a industrie, organizzazioni governative e militari, aziende sanitarie e università. Yarix dispone di uno dei più avanzati Cognitive Security Operations Center in Italia e si avvale di team di persone specializzate in sicurezza difensiva e offensiva, Cyber Threat Intelligence, Incident Response.

Communication & Media Relations Var Group
Sara Lazzeretti
Mail: s.lazzeretti@vargroup.it
Mob. 3391705791

Ufficio stampa
Community
var@community.it
Claudia Laria – 335 790 4158
Andrea Canu – 334 636 7718