VARGROUP

Y-REPORT 2025 - VIII EDIZIONE

HACKTIVISMO: L'ITALIA È STATO IL QUINTO PAESE PIÙ COLPITO NEL 2024

- *97 gruppi di cyber attivisti rilevati da Yarix (Var Group) a livello globale. L'Italia presa di mira da gruppi dell'Asia-Pacifico e filo-russi in occasione del G7 a Kiev;*
- *Ransomware, oltre la metà degli attacchi nel mondo ha riguardato le piccole imprese. In Italia, Lombardia, Emilia Romagna e Veneto tra le regioni più colpite;*
- *Nel 2024, aumentati del 70% tutti gli incidenti di sicurezza e più che triplicati (+269%) quelli di gravità critica. Il Manifatturiero si conferma il settore più esposto;*
- *"Bring Your Own Vulnerable Driver" (BYOVD) e Intelligenza Artificiale per la scrittura di script malevoli tra le tendenze adottate dai cybercriminali.*

Milano, 27 maggio 2025 – **Var Group presenta l'ottava edizione del Y-Report di Yarix,** il suo centro di competenza per la **cybersecurity**, per tracciare lo scenario delle minacce informatiche che hanno colpito l'Italia e il mondo nel corso del 2024.

Nel 2024, il **Security Operation Center** (SOC) di Yarix, sala di controllo da cui vengono monitorati gli attacchi informatici in tempo reale, ha analizzato complessivamente oltre **485 mila eventi di sicurezza** (**+56%** rispetto al 2023), ovvero attività anomale o sospette nei sistemi. **Quasi 1 su 3 di questi eventi (141 mila, +70% sul 2023) è evoluto in incidente,** violazione che ha impattato la sicurezza di dati o sistemi. In questo scenario, **gli incidenti di gravità critica sono più che triplicati** (**+269%** su base annua), trend favorito dalla presenza di vulnerabilità in componenti chiave dell'infrastruttura, come firewall e altri dispositivi di sicurezza.

I due settori più colpiti sono il **Manifatturiero** (12,5%), particolarmente esposto a causa della presenza di ambienti produttivi con dispositivi obsoleti e infrastrutture delocalizzate, spesso caratterizzate da una governance limitata, e l'**IT** (11,8%), per via dell'elevato numero di servizi esposti, soggetti a diverse tipologie di vulnerabilità, e per la natura sensibile dei dati trattati.

Ransomware

Durante il 2024 sono stati mappati **4.721 eventi ransomware** a livello mondiale (+5,5% di rivendicazioni rispetto al 2023), in prevalenza contro PMI (54%), condotti da **92 gruppi ransomware**. Tra questi, **RansomHub** si conferma quello più attivo, contribuendo da solo al 9,80% degli attacchi totali.

L'Italia sale di una posizione e diventa il quarto paese più interessato dai ransomware, dopo Stati Uniti, Regno Unito, Canada e prima della Germania. A livello italiano, gli attacchi ransomware hanno colpito aziende nei settori **Manifatturiero** (32,5%), Consulenza (9%), IT (7,5%), Trasporti (7,5%) e Costruzioni (6,5%), distribuite maggiormente in **Lombardia (30,90%), Emilia-Romagna (15,40%) e Veneto (8,80%).**

Contesto geopolitico e Hacktivismo

L'Italia è stato il 5° Paese più colpito dai gruppi hacktivisti durante il 2024, sia da collettivi filo-russi con motivazioni principalmente legate alla posizione italiana a supporto del governo di

Kiev nel conflitto Russia-Ucraina, come in occasione del primo incontro del 2024 del **G7 da Kiev**, **che da collettivi appartenenti all'area Asia-Pacifico**, volti al sostegno della popolazione palestinese e dunque contrari al sostegno italiano ad Israele. I picchi maggiori sono stati registrati in corrispondenza del **primo e quarto trimestre del 2024.**

Ai primi posti dei paesi più attaccati l'Ucraina, **Israele e la Romania**, quest'ultima per il valore strategico e militare nel conflitto tra Russia e Ucraina. Al quarto posto **l'India**, a causa di dispute territoriali o politiche con i Paesi vicini, per cui è stato identificato un picco di attività da parte di collettivi dell'area Asia-Pacifico.

Il Team di Cyber Intelligence ha registrato **97 gruppi hacktivisti a livello globale,** di cui il più attivo è stato il collettivo filorusso **NoName057, che ha totalizzato più del 55% degli attacchi** per i settori Energia & Utility, Sanità, Banca & Finanza e Trasporti & Logistica.

- **I collettivi allineati con la Russia** hanno concentrato i loro attacchi verso obiettivi ucraini, alleati del governo di Kiev e membri della NATO, giustificando le loro azioni come una risposta al coinvolgimento occidentale nella regione. In altri casi, è stato osservato che gruppi sostenitori del governo di Mosca hanno esteso la loro influenza oltre il conflitto Russia-Ucraina, mostrando sostegno a movimenti interni di alcuni Paesi che hanno causato disagi a livello nazionale (ad esempio la protesta degli agricoltori in Europa) attraverso attacchi DDoS, azioni mirate a sovraccaricare un sito o di un server per renderlo inaccessibile;

- **Gli attori pro-arabi e pro-musulmani** hanno invece mirato a paesi che hanno mostrato supporto politico o militare a Israele nel suo conflitto in corso contro Hamas, considerando gli attacchi DDoS come una forma di ritorsione per il sostegno alle azioni militari del governo di Tel-Aviv. In modo simile, gli attori pro-Palestina e quelli legati ad **Anonymous** hanno indirizzato i loro attacchi verso paesi che consideravano responsabili delle sofferenze dei civili, con particolare attenzione alla situazione di Gaza;

- **Gli hacktivisti dell'area Asia-Pacifico** sono stati coinvolti in azioni relative a dispute tra India e paesi confinanti, come Bangladesh e Pakistan, e nella causa umanitaria scaturita dal conflitto tra Israele e Hamas.

Tendenze 2024: Intelligenza Artificiale nell'attacco e nella difesa

Nel 2024, il team di Incident Response ha gestito **146 compromissioni di sicurezza**, (**+75,9%** rispetto al 2023). Dalle analisi è emerso che l'**Intelligenza Artificiale Generativa è stata impiegata per sviluppare script malevoli**, istruzioni automatizzate per eseguire azioni dannose su un sistema informatico; ciò ha permesso di velocizzare la creazione di malware, permettendo anche ad attori meno esperti di lanciare attacchi, e contribuito a una crescente sofisticazione degli stessi.

Gli attaccanti sono inoltre sempre più abili a cancellare le loro tracce nei sistemi compromessi, rendendo sempre più complesso ricostruire le loro attività e identificare il punto d'ingresso.

Ma l'IA è uno strumento fondamentale anche per la difesa: a un anno dalla nascita di **Egyda**, piattaforma di Yarix che integra **automazione avanzata**, **machine learning** e **intelligenza artificiale** all'interno del SOC, il tempo medio di risposta agli eventi è stato **ridotto di oltre il 50%** grazie a un'elaborazione più rapida e precisa degli alert.

Tra le altre **principali tendenze** osservate dal team:

- l'adozione di **strumenti personalizzati** per la compromissione dei sistemi e l'impiego di **diversi metodi per criptare i dati**, rendendo più difficile il recupero;

- **l'abbassamento della soglia di selezione nei processi di affiliazione**: gruppi come Akira, LockBit, BlackBasta e altri emergenti mostrano un livello di competenze eterogeneo tra i loro affiliati. Questo approccio punta ad aumentare il volume degli attacchi e massimizzare i profitti derivanti dai riscatti;
- **un aumento del 333% di malware progettati per neutralizzare i controlli di sicurezza,** la diffusione di "EDR Killer" per disabilitare i software di sicurezza sugli endpoint (pc, smartphone…);
- l'adozione, da parte di gruppi più evoluti, di metodi sofisticati come il ***"Bring Your Own Vulnerable Driver"*** **(BYOVD),** che installa sul sistema bersaglio un driver legittimo, cioè creati da produttori affidabili, ma contenente vulnerabilità.

Metodologia

Il report offre uno studio dei dati ricevuti e analizzati da parte di Yarix durante il 2024, considerato come periodo di riferimento. Le informazioni provengono da un panel specifico di aziende monitorate dal Security Operation Center e corrispondono alla base clienti di Yarix, che comprende una vasta gamma di settori dell'economia nazionale. Vengono inoltre inclusi i dati relativi alla gestione di incidenti informatici di aziende che non erano precedentemente clienti. Le imprese rappresentate nel panel analizzato hanno in media oltre un migliaio di dipendenti e generano fatturati superiori ai 50 milioni di euro.
I dati sono stati normalizzati statisticamente e resi omogenei al fine di poterli utilizzare come output quantitativo affidabile e in grado di supportare valutazioni qualitative. Tutti i dati raccolti sono stati automaticamente resi anonimi e aggregati per garantire la privacy, eliminando qualsiasi associazione tra le informazioni e le aziende coinvolte.

Var Group

Var Group è l'operatore leader nel settore dei servizi e delle soluzioni digitali, con un fatturato di 823 milioni di Euro al 30 aprile 2024. Grazie alla professionalità delle oltre 3.850 persone, accompagna le imprese nel loro percorso di trasformazione digitale. Ha una presenza territoriale in 13 paesi nel mondo (Italia, Francia, Germania, Spagna, Austria, Svizzera, Albania, Romania, Lettonia, Messico, USA, India e Brasile) 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, Meccanico, Fashion & Luxury, Furniture, GDO & Retail, Finance e Pubblica amministrazione, 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 Collaborative Workspace, Business Applications, Digital Experience, Industry Solutions, Cyber security, Data Science, Digital as a Service, Digital infrastructure, Industrial Digital Twin e Sustainability Solutions.

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 3,2 Miliardi al 30 aprile 2024. 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. Var Group aderisce al Global Compact ONU, ha acquisito la certificazione ambientale ISO 14001 e la certificazione Great Place To Work nel Novembre 2023 e conseguito il rating Ecovadis a livello Silver.

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 oltre 20 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 Operation 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