Primo Piano - *Clusit, incidenti informatici in aumento nel primo semestre 2025: in Italia il 10% degli attacchi a livello mondiale*

Roma - 05 nov 2025 (Prima Notizia 24) **Bersagliati i settori governativo, militare, forze dell'ordine e dei trasporti. Ogni giorno, in media, 15 incidenti gravi nel mondo.**

Nei primi sei mesi del 2025 sono stati 2.755 gli incidenti cyber1 rilevati nel mondo dai ricercatori di Clusit, Associazione Italiana per la Sicurezza Informatica. La tendenza globale del periodo mostra una crescita pari al 36% rispetto al secondo semestre del 2024. Nel nostro Paese, tale aumento si assesta al 13%, con 280 incidenti noti di particolare gravità, che costituiscono da soli il 75% degli eventi rilevati nel 2024. Il totale degli incidenti registrati a livello globale nel primo semestre del 2025 segna un record storico dall'inizio della pubblicazione del Rapporto Clusit, nel 2011. In particolare, negli ultimi cinque anni e mezzo si è assistito a una netta escalation delle attività ostili, con una crescente intensità e frequenza degli eventi: complessivamente, nel periodo che va dal 2020 al primo semestre 2025 sono stati registrati 15.717 incidenti, una cifra pari al 61% di quelli verificatisi a partire dal 20112 . I dati emergono dalla tredicesima edizione del Rapporto Clusit – la seconda nel 2025 - presentata questa mattina in apertura del tradizionale Security Summit Streaming Edition, l'appuntamento di fine anno che riunisce esperti del settore, aziende e professionisti per approfondire i temi più attuali della cybersecurity. I ricercatori di Clusit hanno evidenziato il trend di crescita delle incursioni cibernetiche nel mondo e fornito l'analisi delle nuove minacce, evidenziando le finalità degli attacchi e le tecniche utilizzate, i settori merceologici più colpiti, la gravità degli incidenti censiti e la geografia degli incidenti. Rispetto alla seconda metà del 2024, gli episodi rilevati sono aumentati in modo significativo, passando da una media di 337 a 459 attacchi mensili, oltre 15 al giorno, in media. In crescita, nell'ultimo semestre, anche la gravità degli incidenti: l'impatto medio stimato a livello globale è stato infatti "critico" o "elevato" nell'82% dei casi, contro il 77% del totale nel 2024, dato che nel 2020 si assestava al 50%. Nel nostro Paese - come è stato rilevato dagli autori del Rapporto Clusit - la quota di incidenti con gravità "critica" o "elevata" è stata invece significativamente più bassa che nel resto del mondo, rispettivamente il 7% in Italia, contro 29% nel mondo e il 33% in Italia verso 53% a livello globale. Gli incidenti di gravità "media", al contrario, hanno avuto un'incidenza molto più alta in Italia arrivando a rappresentare il 60% degli incidenti, contro il 18% a livello globale. Ovvero, nel nostro Paese gli attacchi sembrano danneggiare meno che nel resto del mondo: gli incidenti con impatto medio sono molto più numerosi, ma i loro danni risultano circoscritti. "Le analisi dei dati da parte di Clusit, a livello nazionale e globale, mettono in evidenza un marcato squilibrio tra la crescente capacità offensiva degli attaccanti e l'efficacia delle contromisure, purtroppo sempre più a vantaggio degli attaccanti. La difficoltà crescente nel difendersi porta a un aumento significativo dei rischi e, se questa

tendenza dovesse consolidarsi, il problema rischia di espandersi coinvolgendo tutto il sistema organizzativo, industriale e sociale", ha commentato Anna Vaccarelli, presidente di Clusit. Questo, insieme all'incremento delle minacce e della loro gravità, ha portato i ricercatori di Clusit a ribadire che ci troviamo di fronte a una tendenza consolidata e di lungo periodo. Gli stessi notano che, oltre all'allarmante aumento delle attività di matrice criminale, le operazioni condotte dagli Stati, direttamente o tramite gruppi sponsorizzati, sembrano ormai diventate la norma, e vengono implementate in modo sistematico grazie ad un sofisticato arsenale di strumenti offensivi, con diverse finalità ed intensità. "Questo approccio dei cybercriminali" secondo Anna Vaccarelli, "si aggiunge alle tradizionali attività di spionaggio e si concentra su infrastrutture e piattaforme governative, civili e industriali. A ciò si accompagna una persistente attività di disinformazione verso la popolazione, che genera disorientamento e incertezza come mai in passato". Il nostro Paese si colloca tra le nazioni che più risultano incapaci di contenere gli attacchi: nel primo semestre dell'anno, il 10,2% degli incidenti a livello mondiale si è infatti verificato in Italia, contro il 9,9% del 2024, confermando una escalation dal 3,4% del 2021 e dal 7,6% del 2022. I ricercatori di Clusit hanno inoltre evidenziato che nel 2025 l'Italia - rispetto alla media globale - è stata molto più colpita da incidenti di tipo DDoS realizzati da gruppi di sedicenti attivisti che, in realtà, sono molto probabilmente sabotatori coordinati da strutture governative russe. Pur trattandosi di incidenti con impatti di livello tipicamente medio-basso, la loro frequenza, secondo gli esperti, rende necessarie azioni di mitigazione specifiche. "In proporzione al dato globale la percentuale di incidenti realizzati verso il nostro Paese risulta anomala, sia rispetto alla dimensione della popolazione che a quella del PIL nazionale, il che rappresenta uno svantaggio competitivo per il Paese", ha dichiarato Luca Bechelli, del Comitato Direttivo Clusit. Secondo gli Autori del Rapporto Clusit, la crescita in volume degli incidenti nel mondo è sostenuta da un aumento del fenomeno Cybercrime: in valore assoluto, con 2401 incidenti, nel primo semestre del 2025 si è verificato il 76% degli eventi registrati nell'anno 2024. I fenomeni di Espionage/Sabotage e Information Warfare sono invece in calo rispetto al 2024, assestandosi ad una quota di un incidente su 10, a dispetto dell'estensione dei conflitti già attivi nel 2024 e dell'acuirsi delle ulteriori problematiche nel primo semestre dell'anno. Gli esperti di Clusit hanno evidenziato la complessità della reale attribuzione degli attacchi di Information Warfare; le tensioni in corso si riflettono invece in un aumento sostanziale degli incidenti classificabili come Hacktivism, che nei primi sei mesi del 2025 rappresentano, in valore assoluto, il 59% degli eventi di tutto il 2024. Tra quelli avvenuti in Italia nei primi sei mesi del 2025, la maggioranza degli incidenti noti si riferisce proprio alla categoria Hacktivism, che si attesta al 54%, superando a livello nazionale il peso percentuale del Cybercrime. Le organizzazioni italiane risultano particolarmente vulnerabili a iniziative con finalità dimostrativa, di matrice politica o sociale. Il dato riferito ai primi sei mesi del 2025 rappresenta più di una volta e mezza il totale degli incidenti del 2024. Il Cybercrime è stato invece nel nostro Paese la causa del 46% del totale degli incidenti; in questa categoria, si è tuttavia verificato un numero superiore di eventi rispetto a quelli rilevati nello stesso periodo dello scorso anno (130 nel primo semestre 2025 vs 89 nel primo semestre 2024). Gli eventi che hanno colpito con successo più settori contemporaneamente, ovvero rivolti a "Obiettivi Multipli", hanno determinato il 21% delle vittime nel primo

semestre dell’anno corrente e rappresentato oltre l’85% della quantità di incidenti registrati a livello globale nel 2024. Al secondo posto, il settore Governativo / Militare / Forze dell’Ordine, stabile al 14%, con una quantità di incidenti che tuttavia è pari al 75% di quelli registrati nel 2024. Il settore della Sanità, apparentemente in discesa di un punto percentuale rispetto all’anno precedente, con 337 incidenti nel primo semestre del 2025, ha realizzato il 67% dei 500 incidenti registrati nel corso del 2024. In crescita anche la percentuale sul totale degli incidenti anche verso il settore Manifatturiero (dal 6% del 2024 all'8% nel primo semestre 2025): in questo caso, in un solo semestre il comparto ha raggiunto il 90% degli incidenti registrati in tutto il 2024. I settori Professionale /Scientifico /Tecnico e Trasporti /Logistica hanno raggiunto e superato, in soli sei mesi, il numero di incidenti di tutto l’anno precedente: il 94% nel primo caso e addirittura il 110% per il secondo. Anche il settore del Commercio al Dettaglio /Ingrosso si è allineato alla crescita, realizzando oltre il 65% del numero di incidenti dell’anno precedente in soli sei mesi quest’anno. In controtendenza appare il settore Scolastico, in cui si è verificato meno del 50% degli eventi di tutto l’anno precedente. Nel primo semestre di quest’anno i ricercatori di Clusit hanno rilevato un maggior numero di incidenti cyber nell’ambito Governativo / Militare / Forze dell’Ordine italiano, interessato da una quota di eventi pari al 38% del totale, che in valore assoluto si traduce in una quantità di incidenti pari al 279% rispetto all’intero anno precedente. La crescita rispetto allo stesso periodo dello scorso anno è pari a oltre il 600%. Questo dato può essere almeno in parte spiegato con l'aumento della pressione del fenomeno Hacktivism: gli attacchi di tipo dimostrativo, infatti, sono spesso motivati da finalità politiche o geopolitiche e rivolti a vittime nella sfera delle istituzioni pubbliche e militari, in modo tale da generare grande attenzione da parte dell’opinione pubblica, amplificando la visibilità del messaggio che gli attaccanti vogliono veicolare. Al secondo posto, gli incidenti in ambito Trasporti /Logistica (17% del totale), che hanno realizzato in sei mesi oltre una volta e mezzo il numero degli incidenti di tutto l’anno precedente e incrementato l’incidenza sul totale del campione, rispetto all’anno precedente, di 10 punti percentuali. “La crescita degli attacchi nel settore Trasporti e Logistica sembra riconducibile alla volontà degli attaccanti di mettere in crisi interi comparti dipendenti dalle filiere dei fornitori, colpendo più segmenti di mercato contemporaneamente e limitando la capacità di garantire approvvigionamento e distribuzione. Ne sono testimonianza sia l’aumento degli attacchi di matrice attivista tramite tecniche DDOS in questi ambiti, sia le violazioni ai danni di soggetti della supply-chain, che hanno avuto ripercussioni trasversali su numerose organizzazioni del settore", ha commentato Luca Bechelli, del Comitato Direttivo Clusit. Il settore Manifatturiero, in cui è avvenuto il 13% degli incidenti nel primo semestre dell’anno, ha raccolto in Italia una quota più significativa di incidenti rispetto al resto del mondo – che nella vista globale si ferma all’8% - spiegabile, secondo i ricercatori di Clusit, con la peculiarità del tessuto economico del nostro Paese. Il Commercio al Dettaglio /Ingrosso ha registrato in Italia una crescita statisticamente rilevante di incidenti, attestandosi nel semestre su un numero di eventi pari al 70% dei 12 mesi precedenti. A confronto con i dati del 2024, i ricercatori di Clusit segnalano una diminuzione degli incidenti nel settore della Sanità. Le vittime per area geografica Come evidenziato dagli autori del Rapporto Clusit, la lettura della distribuzione geografica delle vittime rende indirettamente la fotografia della digitalizzazione e della normazione sui temi legati alla

cybersecurity nel mondo, nonché di quali siano i Paesi maggiormente presi di mira dalle operazioni cybercriminali. Nel primo semestre 2025, un incidente su quattro è avvenuto in Europa, che ha registrato un calo negli incidenti di 5 punti percentuali rispetto allo scorso anno. Il continente americano si conferma al primo posto per numero di vittime; l'aumento più marcato è stato invece verso il continente asiatico che è cresciuto di sette punti percentuali, raggiungendo il massimo picco mai registrato in questo territorio. Nel solo primo semestre del 2025 in valore assoluto sono stati registrati più incidenti che in tutto il 2024: 523 eventi, pari ad una crescita del 121%. Sono sostanzialmente stabili, invece, Oceania (3%) e Africa (1%). Un quarto degli incidenti registrati nel campione di Clusit nel primo semestre 2025 è stato causato da Malware, che si conferma la tecnica più utilizzata dagli attaccanti. Sebbene questa categoria comprenda molte tipologie di codici malevoli, come illustrato dagli esperti di Clusit, il ransomware è in assoluto quella principale e maggiormente utilizzata grazie anche all'elevata resa economica per gli aggressori. Gli incidenti basati su vulnerabilità, DDoS e Web Attack, costituiscono la seconda tecnica più utilizzata, ma sono cresciuti tuttavia in numero con maggiore rapidità nel primo semestre di questo anno. Nei primi sei mesi del 2025 sono stati infatti la causa di un numero di eventi pari all'83% dell'intero 2024. In valore assoluto i DDoS sono cresciuti in modo più rilevante, realizzando in sei mesi l'84% degli incidenti dell'intero 2024. Il Phishing risulta una tecnica di aggressione stabile rispetto al 2024, confermandosi causa dell'8% degli attacchi nel mondo; è diminuito l'utilizzo di Tecniche Multiple (da 5% a 3%) e Identity Theft / Account Cracking (-3 punti percentuali). Un'ipotesi plausibile di questo fenomeno, secondo gli autori del Rapporto Clusit, potrebbe essere la contemporanea spinta di norme che richiedono formazione continua per tutti gli operatori, l'adozione di strumenti efficaci di gestione delle identità (Multi Factor Authenticantion in primis e, rispetto a quest'ultima, una maggior presenza di questa caratteristica in servizi enterprise), con una maggiore disponibilità a adottare queste soluzioni da parte di molte organizzazioni, consce di quanto il rischio sia alto, ma mitigabile. I ricercatori di Clusit hanno inoltre evidenziato che i Web Attack, pur continuando a rappresentare la percentuale minore delle tecniche prese in esame nel campione, nel primo semestre 2025 hanno superato in valore assoluto la somma degli eventi dell'intero 2024. La tecnica prevalente causa degli incidenti in Italia nel primo semestre del 2025 è stata quella dei DDoS, (54%), con un peso significativamente maggiore rispetto a quello occupato a livello globale, dove costituiscono solo il 9% del totale. I ricercatori di Clusit hanno evidenziato in questo caso la correlazione con gli incidenti causati da campagne di Hacktivism: molto spesso la tecnica di attacco utilizzata dagli hacktivist è proprio il DDoS, poiché si punta a interrompere l'operatività di servizio dell'organizzazione o istituzione individuata come vittima. Lo scopo degli hacktivist è di innalzare l'attenzione sulla causa supportata e l'interruzione di servizi basati su internet può essere un mezzo efficace per rendere evidente al pubblico il proprio messaggio di denuncia o protesta. Seguono, nel nostro Paese, le tecniche basate su Malware, con il 20% degli eventi, su Vulnerabilità (5%), e tecniche di Phishing /Social Engineering (4%). All'analisi degli attacchi nel mondo e in Italia nel primo semestre del 2025 seguono all'interno del Rapporto Clusit le rilevazioni e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica, che offrono dati e informazioni su attività ed operazioni svolte nel corso dei primi sei mesi dell'anno. I dati e l'analisi

sull’evoluzione della Cybersecurity in ambito manifatturiero/industriale, tratti dalle ultime rilevazioni Clusit al 30 giugno 2025, completano lo scenario. Segue poi un approfondimento su Conformità alla NIS2 e CyberSecurity OT, a cura di Enzo M. Tieghi e Mario Testino, e uno Speciale Intelligenza Artificiale: Intelligenza Artificiale (IA) agentica: quali evoluzioni ci attendono nella cybersecurity, a cura di Federica Maria Rita Livelli; L’uso dei sistemi di AI generativa gratuiti nella gestione del ciclo di vita dei requisiti normativi, a cura di Giancarlo Butti. Il Rapporto Clusit contiene inoltre la seconda edizione della survey sulla Cybersecurity nelle micro e piccole/medie imprese, realizzata nel 2025 dalla Camera di Commercio di Modena in collaborazione con l’Università di Modena e Reggio Emilia e con Clusit. La sezione Focus On si concentra poi sull’approfondimento di alcuni temi: Cybersecurity nei sistemi portuali: dall’esigenza di adeguamento alla resilienza sistemica, a cura del Centro di Competenza Start 4.0 e dell’Autorità di Sistema Portuale del Mar Ligure Occidentale; Sicurezza delle applicazioni cloud: visibilità e controllo continuo dell’ecosistema SaaS, a cura di CrowdStrike; Analisi degli incidenti Cyber nel settore culturale italiano tra il 2020 e il 2024, a cura di Joram Marino e Federica Vennitti; Noi e i nostri dati In Rete: un universo da scoprire, a cura di Andrea Ru.i

(Prima Notizia 24) Mercoledì 05 Novembre 2025