



Attacchi digitali in Italia: i macro trend emersi dalle indagini OAD di AIPSI

A cura di: Marco Rodolfo Alessandro Bozzetti 🕒 25 Gennaio 2024


OAD, Osservatorio Attacchi Digitali in Italia, è l'unica indagine on line via web in Italia sugli attacchi digitali intenzionali ai sistemi informatici di aziende ed enti operanti in Italia, e sulle misure di sicurezza tecniche ed organizzative presenti



L'indagine OAD in tutti questi anni è stata operativamente realizzata da **Malabo Srl** (www.malaboadvisoring.it), la società di consulenza direzionale sull'ICT (Information and Communication Technologies) che implementa l'indagine online, elabora i dati raccolti e stende il rapporto finale, sotto la guida di **AIPSI**, Associazione Italiana Professionisti Sicurezza Digitale, capitolo italiano di ISSA (www.aipsi.org, www.issa.org), che imposta e supporta l'iniziativa, pubblica il rapporto finale dell'indagine e ne garantisce la **qualità** e l'**indipendenza** dell'analisi e dei contenuti anche dagli Sponsor.

L'indagine è rivolta liberamente e in maniera anonima ad aziende/enti di ogni settore merceologico, incluse le Pubbliche Amministrazioni Centrali e Locali, e di ogni dimensione (come numero di dipendenti e fatturato/giro d'affari). OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un sistema informativo di una azienda/ente, un pieno e libero accesso al questionario online con risposte preimpostate in maniera **totalmente anonima**. Essendo libero l'accesso ai questionari online su Internet, il campione che emerge non ha stretta valenza statistica ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico delle aziende/enti dei rispondenti, esso fornisce precise ed interessanti indicazioni sul fenomeno degli attacchi digitali in Italia, soprattutto per le piccole e piccolissime organizzazioni, che in Italia sono la stragrande maggioranza (dati ISTAT per le aziende italiane: 99,91% le PMI con meno di 250 dipendenti, e di queste circa 95% con meno di 10 dipendenti) e che difficilmente sono considerate nelle altre indagini nazionali ed internazionali.

Obiettivo principale di OAD è analizzare anno per anno sia il fenomeno degli attacchi digitali intenzionali nella realtà italiana, sia le misure di sicurezza digitale poste in esercizio sui sistemi informativi delle aziende/enti rispondenti al questionario. Il questionario online ed il Rapporto finale pubblicato da AIPSI sono inoltre due efficaci strumenti per creare e diffondere la conoscenza e la "cultura" della sicurezza digitale in Italia.

Con il Rapporto OAD 2023, l'ultimo pubblicato (è in allegato, liberamente scaricabile, alla pagina <https://www.aipsi.org/eventi/eventi-in-programma/902-aipsi-ha-pubblicato-il-rapporto-oad-2023-ora-scaricabile.html>), l'iniziativa OAD  raggiunge il sedicesimo anno di indagini consecutive, avvalendosi della preziosa

collaborazione della Polizia Postale e delle Telecomunicazioni che ha sempre fornito dati e informazioni sul crimine informatico.

La fig. 1 mostra le copertine dei vari Rapporti pubblicati, tutti scaricabili dal sito ad hoc realizzato quale repository sia dei rapporti sia della documentazione, e in certi casi degli streaming video, degli eventi realizzati anno per anno per la presentazione dei risultati delle indagini: <https://www.oadweb.it/it/rapporti-e-relativi-convegni.html>.

L'indagine, ed i relativi Rapporti, fino all'edizione del 2015 erano indicati come OAI, Osservatorio Attacchi Informatici in Italia, e dal 2016 l'acronimo è stato cambiato in OAD, per meglio evidenziare la copertura dell'indagine a tutto il mondo digitale.



Fig. 1

L'autore in questo articolo analizza e commenta l'evoluzione degli attacchi più diffusi indicati nei questionari online nel corso delle varie edizioni OAD/OAI.

L'analisi ed i commenti sull'evoluzione delle misure tecniche ed organizzative che le aziende/enti rispondenti hanno dichiarato compilando anno per anno il



questionario online saranno oggetto di un successivo articolo.

L'evoluzione degli attacchi digitali e della loro diffusione in Italia dalle indagini OAD

La fig. 2 mostra l'andamento in percentuale degli attacchi digitali rilevati dalle/dai rispondenti al questionario dal 2007 al 2022.

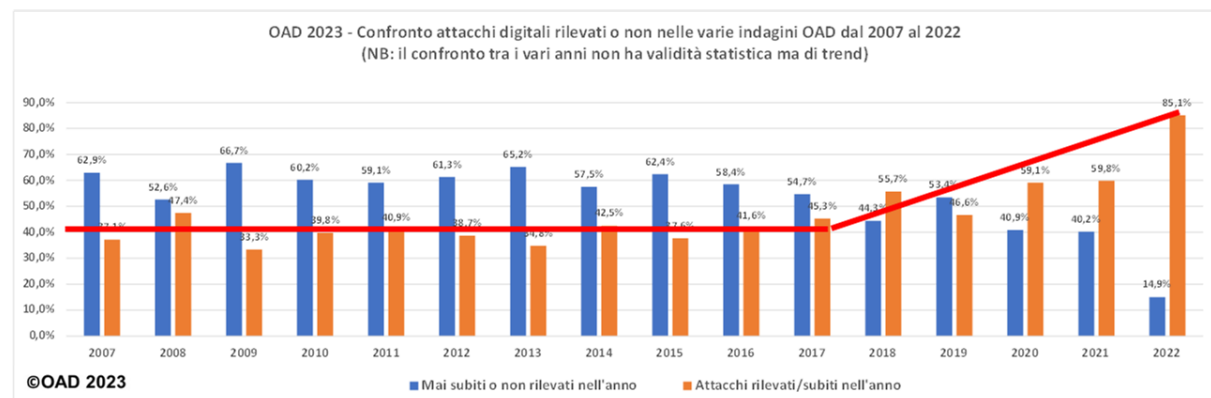


Fig. 2

La barra arancione evidenzia la percentuale degli **attacchi rilevati** anno per anno dai rispondenti. Essendo questo bacino diverso anno per anno, i dati percentuali mostrati non sono strettamente confrontabili da un punto di vista statistico, ma forniscono una chiara indicazione del trend degli attacchi, trend per altro confermato da tutte le altre indagini a livello nazionale ed internazionale sul tema.

La riga rossa sulla fig. 2 evidenzia come dal 2007 al 2016 gli attacchi rilevati si attestano attorno al 40%, con variazioni ad onda tipiche della seguente logica: dopo un incremento della diffusione di attacchi, vengono poste in atto miglioramenti/potenziamenti delle misure di sicurezza a contrasto. Poi, nella continua rincorsa tra guardie e ladri, negli anni successivi gli attaccanti trovano nuove modalità per colpire, cui seguono ulteriori potenziamenti delle misure di sicurezza. In questo primo periodo, un picco di attacchi nel 2008, uno dei primi "annus horribilis". Dal 2017 la percentuale di attacchi inizia a crescere, e nel 2018 si verifica la prima svolta tra i rispondenti: la percentuale di attacchi rilevati supera quella degli attacchi non subiti (o non rilevati). **Dal 2020 questa crescita è in continua forte crescita, e raggiunge il picco nel 2022.**



Le cause di questa crescita sono presto dette. Oltre agli attacchi che possiamo far rientrare nella “tradizionale” criminalità informatica, nel 2020 scoppia in Italia l’epidemia del Covid-19 che porta, in pochi giorni, la gran parte dei lavoratori di imprese pubbliche e private a lavorare da remoto via Internet: molti dei sistemi informativi, soprattutto delle piccole e medie organizzazioni, e dei dispositivi d’utente (sovente di proprietà degli stessi utenti, il BYOD, Bring Your Own Device), non avevano strumenti di sicurezza adeguati, e tanto meno erano adeguate le misure organizzative e le competenze degli utenti per lavorare da remoto. Questo ha enormemente ampliato l’area di vulnerabilità informatica, ed ha causato un incremento degli attacchi, con l’aiuto anche di numerosi siti malevoli sul Covid 19 e sulle vaccinazioni; su questi siti malevoli non solo false informazioni, ma anche varie trappole informatiche per catturare identità digitali, informazioni sulle carte di credito, diffusione di malware, etc.

Il 2022 evidenzia un ulteriore forte incremento degli attacchi digitali, che raggiunge come diffusione il picco assoluto dell’**85,1%** dei sistemi informativi delle aziende/enti rispondenti al questionario OAD. Oltre alla coda di attacchi che fanno riferimento al Covid, nel 2022 l’attacco della Federazione Russa all’Ucraina scatena un largo uso di attacchi digitali ai principali sistemi informativi di enti pubblici e privati non solo dell’Ucraina ma anche dei vari paesi occidentali chi si sono affiancati all’Ucraina del respingere questa invasione. La guerra cibernetica che si affianca alla guerra sul campo non è una novità del 2022, e da tempo è di fatto in atto contro le democrazie liberali occidentali da parte di paesi comunisti come Cina, Russia, Corea del Nord e da certi paesi islamici, in particolare dall’Iran. Il Rapporto OAD 2023 approfondisce questo argomento, ed elenca i principali attacchi nel 2022, a livello mondiale ed italiano, riconducibili anche alle guerre digitali.

Quali i **tipi di attacco digitali più diffusi** tra quelli subiti e rilevati dalle aziende/enti rispondenti tra il 2007 ed il 2022? La fig. 3 confronta anno per anno i **tre attacchi più diffusi**.

| Tipologia attacchi più diffusi tra i rispondenti (%) | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 (1) | 2022 |
|--|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|----------|-------|
| Distruzione s/o compromissione FISCA di dispositivi ICT fissi o di loro parti | | | | | | | | | | | | | 25,2% | | | |
| FURTO dispositivi fissi ICT o di loro parti | 44,0% | 50,0% | 37,4% | 29,6% | 33,8% | 44,4% | | | 34,0% | 33,3% | | | 28,2% | | | |
| FURTO di dispositivi ICT mobili di proprietà dell'azienda/ente e in uso presso i suoi dipendenti/collaboratori | | | | | | | | | | | | | | | | |
| FURTO INFORMAZIONI da singoli specifici sistemi fissi ICT (PC, server, storage system, etc.) del Sistema Informativo, anche terzianizzati/in cloud | | | | | | | | | | | | | | | | |
| FURTO INFORMAZIONI relative all'azienda/ente da sistemi MOBILI (palmari, smartphone, tablet, ecc.) sia di proprietà dell'azienda/ente sia dell'utente finale (BYOD) | | | | | | | | | | | | | | | | |
| Attacchi all'identificazione, autenticazione e controllo accessi degli utenti finali e privilegiati | | | | | | | | | | | 39,4% | 54,2% | 34,0% | 30,0% | 27,6% | 23,5% |
| Attacchi alle reti locali e geografiche, fisse e wireless, inclusi i collegamenti ad Internet, e ai DNS | 40,0% | | | | | | | | | 44,6% | 27,2% | 34,7% | | 28,7% | 25,9% | |
| Attacco s/o uso non autorizzato di sistemi IT nel loro complesso (dal PC agli host fisici o virtuali), anche terzianizzati | | | | | | | | | | | | | | | | |
| MODIFICHE malevoli s/o non autorizzate ai programmi applicativi e alle loro configurazioni, del Sistema Informativo anche terzianizzate e in cloud | | | | | | | | | | | | | | | | |
| MODIFICHE malevoli s/o non autorizzate alle INFORMAZIONI trattate dalle applicazioni del Sistema Informativo, anche quelle terzianizzate/in cloud | | | | | | | | | | | | | | | | |
| SATURAZIONE (DoS, DDoS) risorse digitali del Sistema Informativo, anche quelle terzianizzate/in cloud | | | | | | | 38,8% | 42,5% | | | 29,2% | | | | | 19,6% |
| Attacchi ai propri sistemi/server digitali in CLOUD o comunque TERZIANIZZATI presso fornitori terzi | | | | | | | | | | 21,5% | | | | 17,6% | 17,6% | |
| Attacchi a dispositivi dei sistemi OT, Operational Technology, tra inclusi i sistemi IoT, i sistemi per l'automazione industriale (SCADA, DCS, PLC, ...) e la robotica | | | | | | | | | | | | | | | | |
| Nel corso dell'intero 2022 il Sistema Informativo ha subito attacchi digitali la cui tipologia non è stata individuata | | | | | | | | | | | | | | | | |
| Utilizzo codici maligni (malware) sia a livello di posto di lavoro che di server | 76,5% | 84,3% | 59,0% | 47,0% | 66,2% | 64,8% | 65,1% | 67,0% | 70,4% | | | | | | | |
| Attacchi di Social Engineering e di Phishing | 58,0% | 32,0% | 27,0% | 50,0% | 46,5% | 65,8% | 67,1% | 71,9% | | | | | | | | |

Si deve considerare che solo dall'edizione del 2018 OAD separa nettamente nel questionario, e quindi nel rapporto finale, la tipologia di attacchi, ossia cosa si attacca, dalle tecniche di attacco usate[1]: nei questionari precedenti tale chiara distinzione non esisteva, e come mostrato nelle ultime due righe in corsivo della tabella in fig. 3 dal 2007 al 2016 i codici maligni, che sono una famiglia di tecniche di attacco che include anche il ransomware, sono al primo posto tra gli attacchi, e la raccolta non autorizzata di informazioni, come il social engineering, altra famiglia di tecniche di attacco, è quasi sempre al secondo posto.

Sempre in questo arco temporale, nelle domande del questionario online non veniva distinto il furto di apparati ICT fissi da quelli mobili: il valore percentuale riportato nella figura accomuna quindi questo tipo di attacco, che viene distinto tra apparati fissi e mobili solo dal 2017.

La Tabella in fig. 3 volutamente, per motivi di chiarezza e leggibilità, non riporta tutte le percentuali di diffusione degli altri attacchi, che sono visibili nei vari rapporti pubblicati (si veda <https://www.oadweb.it/it/rapporti-e-relativi-convegni.html>).

Il furto di dispositivi "fisici" mobili o fissi (o di alcune loro parti) rientra ai primi tre posti come diffusione fino al 2019, per poi scendere nella classifica negli anni successivi ma senza mai sparire o raggiungere percentuali insignificanti. Il motivo per il furto di cellulari è abbastanza scontato: da un lato gli smartphone di buone capacità hanno un costo elevato, e quindi anche l'usato ha un suo mercato significativo. Dall'altro contengono normalmente userid e password di tutti gli account del possessore, che sovente non cripta tali informazioni: il furto del cellulare consente al ladro di disporre di tali informazioni per compiere attacchi ben più gravi, come ad esempio bonifici sui conti correnti del possessore. Solo da pochi anni gli istituti bancari e finanziari hanno introdotto l'autenticazione a più fattori, ad esempio con OTP inviate sul cellulare, che hanno significativamente ridotto la possibilità di questi tipi di attacchi. Nonostante questo il furto dell'identità digitale degli utenti rimane uno degli attacchi più diffusi, attuato prevalentemente con attacchi di social engineering (si veda fig. 4 e i relativi commenti). Ai primi tre posti si posizionano anche gli attacchi alle reti di comunicazione, soprattutto alle connessioni ad Internet, ma non negli ultimi quattro anni di indagine; i provider hanno potenziato le misure di sicurezza, soprattutto in ottemperanza alla direttiva europea NIS, emessa nel



2016, ora aggiornata con la NIS2[2].

Un altro tipo di attacco, la saturazione delle risorse ICT collegate ad Internet (DoS/DDoS, Denial of Service/Distributed DoS), entrò come terzo in termini di diffusione tra le/i rispondenti nel 2013 e nel 2014, e si è riposizionato a questo posto anche nel 2022, dato che molti attacchi da parte russa nell’ambito della guerra ibrida contro l’Ucraina sono di questo tipo.

Nel 2022 il primo posto come attacco più diffuso è stato guadagnato dalle “Modifiche malevoli e/o non autorizzate ai programmi applicativi e alle loro configurazioni del Sistema Informativo, anche terzarizzate e in cloud”, che negli anni precedenti non era mai entrato tra i primi tre: questo indica che gli attacchi sono sempre più mirati e critici, e sono in grado di cambiare, in maniera malevole, le configurazioni dei sistemi ICT e delle loro applicazioni. Questa tipologia di attacco è attuata prevalentemente con molteplici tecniche, anche in contemporanea, e con sofisticati malware. La fig. 4 evidenzia che proprio nel 2022 le tecniche ATP sono state le più diffuse, seguite da script-malware e da social engineering, almeno per gli attacchi rilevatesi più critici.

La citata fig. 4 mostra le sette famiglie di tecniche di attacco (considerate separatamente dalle tipologie di attacco dal 2018), e riporta non le specifiche percentuali di diffusione ma la loro graduatoria nelle prime tre posizioni, considerando il loro livello di diffusione percentuale nell’attacco con i maggiori e più gravi danni per il sistema informativo oggetto delle risposte al questionario OAD.

| Tecniche di attacco più diffuse tra i rispondenti per gli attacchi più gravi rilevati (%) | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|--|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| Attacco fisico | | | | | | | | | | | | | | 3* | 3* | |
| Raccolta informazioni non autorizzata (es. social engineering, phishing, pharming, hoax, scanning, ecc.) | | 2* | 2* | 2* | 2* | 2* | 2* | 2* | 2* | | | | 2* | 1* | 1* | 2* |
| Script e programmi maligni (ransomware, spyware, adware, ...) | 1* | 1* | 1* | 1* | 1* | 1* | 1* | 1* | 1* | | 1* | 1* | 3* | 2* | 2* | 3* |
| Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm | | | | | | | | | | | 2* | 2* | | | | |
| Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metasploit, ...) | | | | | | | | | | | 3* | 3* | 1* | | | |
| Strumenti distribuiti controllati centralmente (Command Control) quali botnet | | | | | | | | | | | | | | | | |
| Utilizzo di due o più delle precedenti tecniche (ivi incluso APT, Advanced Persistent Threat) | | | | | | | | | | | | | | | | 1* |

Fig. 4

Nella fig. 4 gli anni dal 2007 al 2016 sono evidenziati con un sottofondo grigio, e riprendono i dati in corsivo della fig. 3. Volutamente nella fig. 4 non si sono riportate le specifiche percentuali, dato che negli anni successivi sono state calcolate e pubblicate con diverse logiche[3]: si è preferito quindi indicare solo il posizionamento nei primi tre posti, anno per anno, delle singole famiglie di



tecniche.

Nell’arco temporale 2007-2022 la famiglia “script-codici maligni” è quasi sempre al primo posto, seguita dalla famiglia di tecniche “social engineering”. La ben nota larga diffusione in Italia di malware, e in particolare di ransomware, è dovuta in particolare dal non tempestivo e sistematico aggiornamento dei software in produzione e dalla non completa e sistematica attuazione di backup. Sovente le piccole organizzazioni non rinnovano i contratti di manutenzione coi fornitori di software e non installano le patch ed i fix dei programmi, sia per risparmiare sia perché non hanno la competenza ed il tempo per seguire tutti gli aggiornamenti: il che porta al permanere di vulnerabilità facilmente sfruttabili dagli attaccanti. Il riscontro a questi problemi è dato dalla rilevazione delle misure di sicurezza in essere effettuata da OAD nei vari anni, con alcuni dati e considerazioni che saranno l’oggetto di un prossimo articolo. La raccolta malevole di informazioni, tipicamente il social engineering, è causata dalla scarsa sensibilità e formazione sul corretto e sicuro uso dei sistemi informativi da parte della loro utenza. Non a caso nelle indagini europee DESI[4] l’Italia è agli ultimi posti, ed è in assoluto l’ultima in termini di specifiche competenze ICT. Per un approfondimento si veda il Cap. 3.3.2 del Rapporto OAD 2023. Nel 2020 e 2021 al terzo posto risultano gli attacchi “fisici”, intenzionali e distruttivi ai sistemi ICT: oltre alla distruzione o danneggiamento fisico ad alcuni dispositivi ICT, tipicamente quelli periferici negli uffici (dagli switch alle stampanti condivise, per favore un esempio) in questa famiglia è incluso anche l’uso malevolo di chiavette USB per copiare file e dati dai sistemi. E’ un attacco “fisico” facilitato dal non blocco delle porte USB soprattutto su server e dispositivi “periferici”.

Il forte incremento di attacchi digitali rilevato dalle indagini OAD è confermato dai **dati forniti dalla Polizia Postale e delle Comunicazioni**. Per le sole **infrastrutture critiche italiane**, lo specifico gruppo della Polizia Postale C.N.A.I.P.I.C. ha rilevato un moltiplicarsi degli attacchi rispetto agli anni precedenti, come evidenziato dalla fig. 5. La Polizia Postale evidenzia forti incrementi anche nelle frodi informatiche, nelle truffe online e nella prevenzione del cyberterrorismo per il 2022, come dettagliato nel Capitolo 8 del Rapporto OAD 2023 cui si rimanda per approfondimenti.

| Protezione strutture critiche | 1 gen - 31 dic 2022 | 1 gen - 30 apr 2021 | 1 gen - 31 dic 2020 | 1 gen - 31 dic 2019 | 1 gen - 31 dic 2018 | 1 gen - 31 dic 2017 | 1 gen - 31 dic 2016 |
|-------------------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| Attacchi rilevati | 13.099 | 282 | 509 | 1181 | 459 | 1.032 | 844 |
| Alert diramati | 113.420 | 24.824 | 83.416 | 82.484 | 80.777 | 31.524 | 6.721 |
| Indagini avviate | 110 | 34 | 103 | 155 | 74 | 72 | 70 |



| | | | | | | | |
|--|------|------|------|------|------|-------|-------|
| Persone arrestate | n.d. | n.d. | n.d. | 3 | 1 | 3 | 3 |
| Persone denunciate/indagate | 334 | n.d. | 105 | 117 | 14 | 1.316 | 1.226 |
| Perquisizioni | n.d. | n.d. | n.d. | n.d. | n.d. | 73 | 58 |
| Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest) | 77 | 17 | 69 | 79 | 108 | 83 | 85 |

Fig. 5 (Fonte: elaborazione OAD su dati Polizia Postale)

Legenda: n.d. = non disponibile, il dato non è stato fornito

Analizzando quali settori merceologici sono stati i più colpiti dagli attacchi digitali, emerge, come è ragionevole, che quelli percentualmente più colpiti sono le organizzazioni di grandi dimensioni e con elevati guadagni e flussi finanziari. I criminali informatici attaccano i ricchi, non i poveri: le fig. 6 e 7 lo evidenziano rispettivamente in termini di dimensioni, come numero di dipendenti e in termini di fatturato per le aziende/enti rispondenti. La fig. 7 conferma quanto indicato nella fig. 6, anche se 1/3 delle aziende/enti rispondenti non ha voluto indicare la classe del loro fatturato.

E' bene sottolineare come le percentuali emerse e indicate nelle due figure dipendano fortemente da quanti hanno risposto al questionario, appartenenti alle diverse classi considerate. Come già evidenziato, questi dati hanno soprattutto validità nelle indicazioni/trend sui fenomeni riguardanti gli attacchi digitali in Italia: e questo vale anche per tutte le percentuali elaborate nei diversi rapporti OAD.

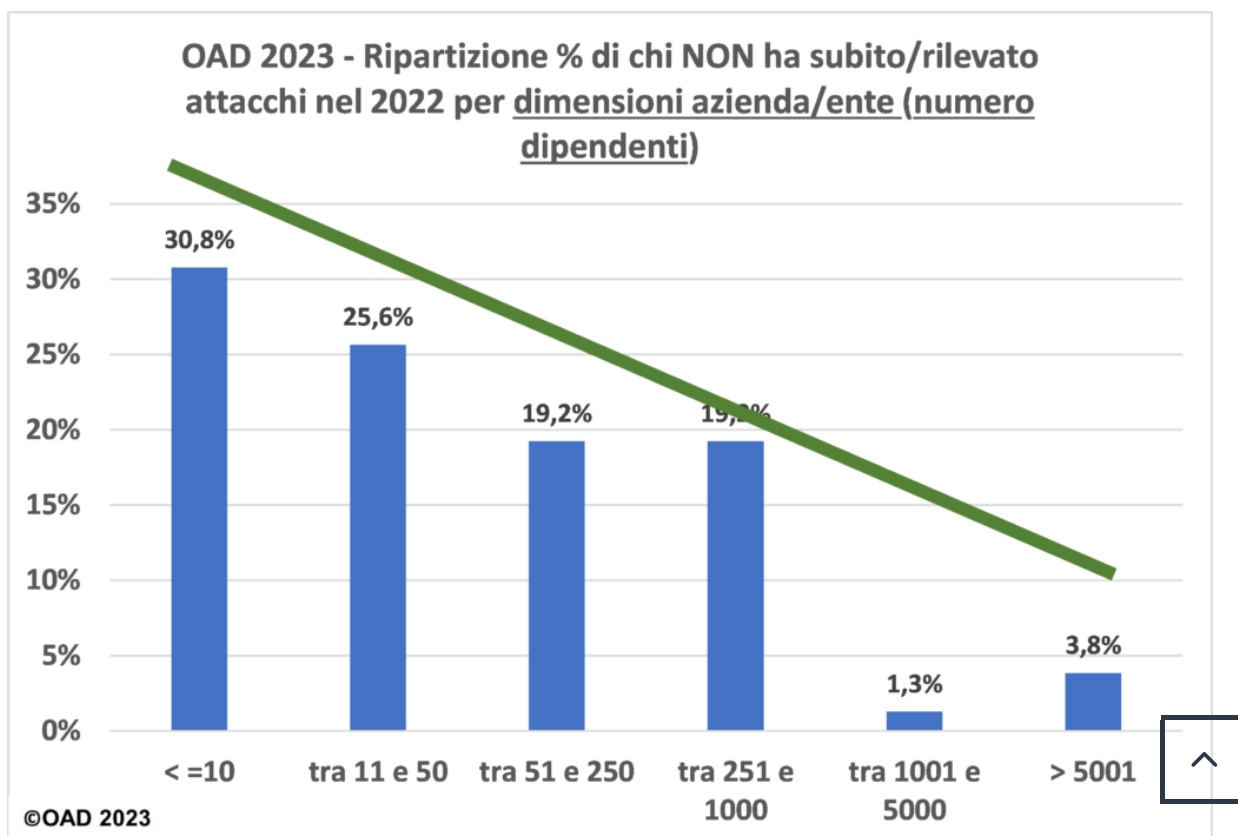


Fig. 6

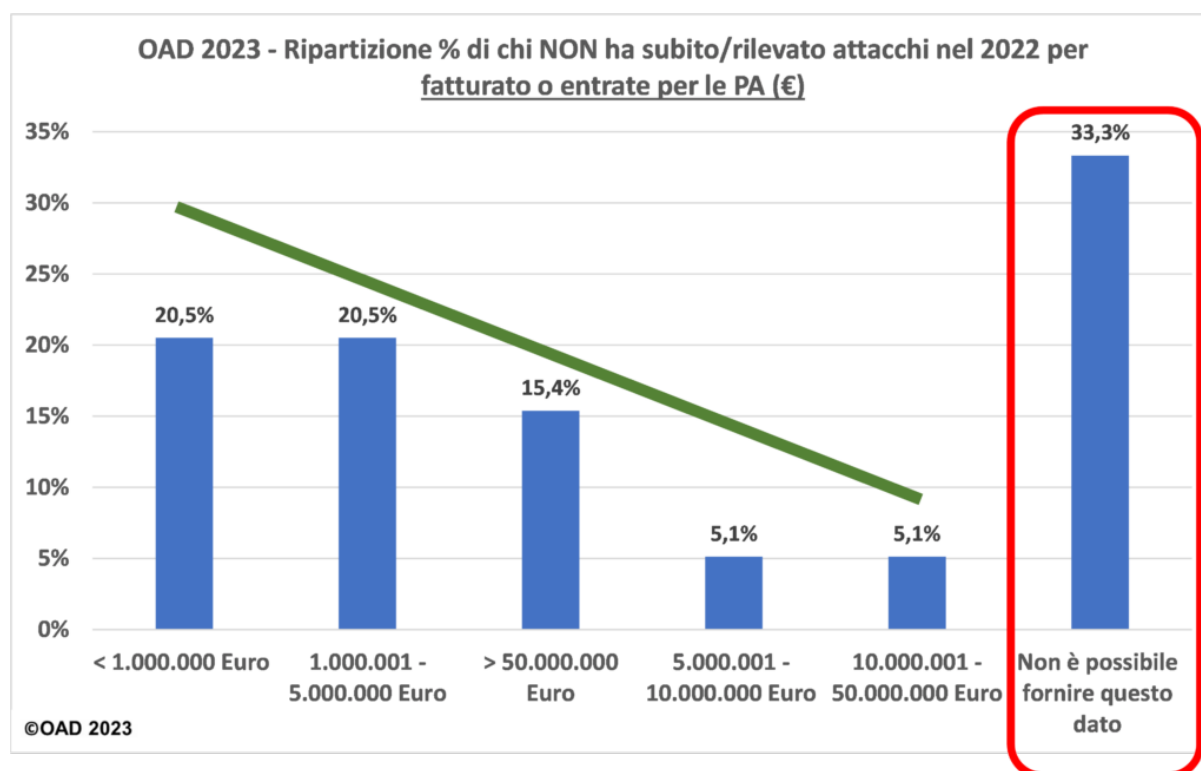


Fig. 7

Nel tempo inoltre gli impatti degli attacchi subiti hanno avuto impatti sempre più gravi. Nelle ultime edizioni OAD gli impatti più gravi sono suddivisi tra **impatti tecnici**, in termini di **durata del disservizio**, ed **impatti economici**, come ulteriori **costi sul budget** del sistema informativo ed il loro più o meno forte ripercuotersi sul bilancio complessivo dell'azienda/ente rispondente. Ad esempio per l'ultima edizione 2023, l'impatto tecnico è stato alto e significativo per il 73,6% delle aziende/enti rispondenti, con un disservizio durato **più di 2 giorni**, in ambito informatico un tempo veramente lungo. Una così alta percentuale è ancor più preoccupante in quanto emerge da aziende ed enti mediamente con misure di sicurezza digitali di buon livello e allo stato dell'arte, come verrà approfondito nel prossimo articolo. L'impatto economico ha visto un significativo aumento dei costi a livello di budget del sistema informativo (utilizzo di nuovi strumenti e servizi di sicurezza, formazione utenti e specialisti, consulenze tecniche e legali, comunicazioni coi media, etc.). **L'impatto economico** è oramai **elevato e significativo** per circa ¼ delle aziende/enti rispondenti, i cui ulteriori costi tecnici si ripercuotono fortemente sul bilancio dell'intera azienda/ente. Queste percentuali sono crescite nelle diverse edizioni di OAD, e confermano una volta di più la pericolosità e la criticità crescente



degli attacchi digitali subiti.

Le probabili **motivazioni per un attacco digitale** vedono sempre ai primi posti, in tutte le indagini OAD/OAI, **motivazione economiche**, declinate tra varie voci quali, in primis, **frode e ricatto**. Percentuali non trascurabili, seppur con forti differenze nelle diverse edizioni, fanno riferimento anche al **sabotaggio** e all'**hacktivism**.

Come esempio la fig. 8 riporta le motivazioni probabili per l'attacco più grave rilevato per l'indagine OAD 2023. In questo grafico emerge la voce **guerra digitale**, con un importante 11,5%, indice del forte impatto dell'invasione della Ucraina. Tale voce era già presente nei questionari delle edizioni precedenti, ma aveva sempre raccolto percentuali trascurabili.

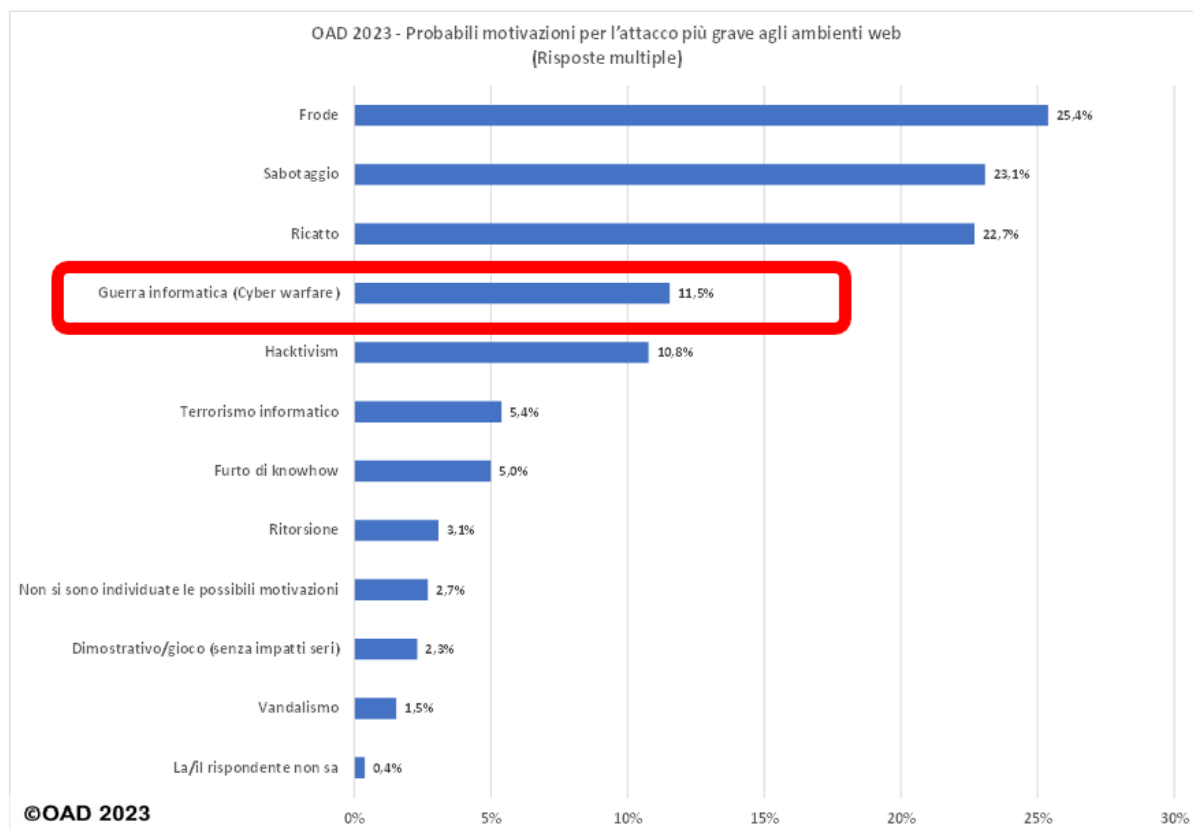


Fig. 8

I probabili **attaccanti per l'attacco più grave** sono man mano cambiati nel tempo, ed evidenziati nei diversi rapporti pubblicati. Nei primi anni di OAI e poi OAD, percentuali significative erano per attori interni all'azienda/ente colpita, che man mano sono stati raggiunti e poi superati percentualmente dagli attori "esterni", coi quali collaborano talvolta utenti interni, volontariamente o



involontariamente: tipiche attività sono ad esempio l'apertura di email di phishing, l'accesso a siti malevoli, il fornire il proprio account ad un collega o a un interlocutore.

La **prima conclusione** che emerge dall'analisi dei trend di OAD negli anni, e che conferma quanto indicato anche a livello europeo e mondiale dalle più autorevoli indagini, quali quelle dell'ENISA e del World Economic Forum (si rimanda per approfondimenti al Cap. 3 del Rapporto OAD 2023), è la **forte diffusione**, anche in Italia, **di attacchi digitali che portano gravi impatti** alle aziende/enti che li subiscono.

Tale gravità aumenta considerando come le aziende/enti rispondenti ai questionari online di OAD sono dotate, in maggioranza, di idonee misure di sicurezza tecniche ed organizzative: si rimanda al prossimo articolo l'approfondimento di questo tema.

D'altro canto in Italia le piccole e piccolissime organizzazioni, sia di imprese pubbliche che private, costituiscono in Italia la stragrande maggioranza (per le aziende 99,91% le PMI, circa 95% quelle con meno di 10 dipendenti, si veda Cap.): esse non possono disporre al loro interno, salvo le dovute eccezioni, delle opportune competenze per impostare e gestire le idonee ed aggiornate misure di sicurezza. Devono rivolgersi a esperti e a servizi esterni, quali ad esempio **MSS**, Managed Security Services, e **CSaaS**, CyberSecurity as a Service.

Ma **come scegliere correttamente** tra le varie offerte e le varie pubblicità, se non si hanno nemmeno le minime competenze per decidere in merito alla sicurezza digitale? E' il solito dilemma nella scelta di un "buon" professionista (medico, avvocato, commercialista, etc.), aggravato in questo contesto dalla incompetenza spesso totale sulla sicurezza digitale, purtroppo per l'Italia confermata anche dal già citato indice DESI.

La **sfida, e la soluzione**, per ridurre il numero di attacchi che vanno a buon fine e con forti impatti sulla continuità operativa e sui conti economici è proprio la **diffusione delle competenze di base sulla sicurezza digitale** non solo per gli utenti dei sistemi informativi, ma anche su chi decide in merito, tipicamente il vertice dell'azienda/ente. In questa ottica sono significative le azioni di libere



autorevoli associazioni, quali AIPSI, e di qualificate riviste come ICT Security Magazine: ma ancora molta strada rimane da fare!

Cosa ci riserva il prossimo futuro? Quasi sicuramente un continuo incremento sia del numero di attacchi digitali sia dei gravi impatti sulle organizzazioni attaccate: oltre alla "tradizionale" criminalità digitale, un aumento di fake news e di attacchi per hactivism e cyber warfare, dovuti soprattutto all'aggravarsi dell'instabilità geopolitica e del chiaro e forte attacco alle democrazie liberali occidentali da parte di paesi illiberali e/o islamici-teocratici. Vedremo la conferma, o non, di questa tendenza anche con la prossima edizione dell'indagine, OAD 2024, le cui prime attività sono iniziate in AIPSI, si veda: <https://www.aipsi.org/eventi/eventi-in-programma/916-l-iniziativa-oad-2024-di-aipsi.html>

Note

[1] Per approfondimenti si rimanda all'**Allegato 2.2** del Rapporto OAD 2023

[2] La direttiva europea NIS (UE 2016/1148), sostituita dalla NIS2 (UE 2022/2555) entrata in vigore nel 2023, dettano le misure di sicurezza digitale che i gestori di infrastrutture critiche e servizi essenziali di ogni paese europeo devono implementare, con l'obiettivo di potenziare e omogenizzare il livello di sicurezza digitale dell'intera Unione Europea. Si veda <https://eur-lex.europa.eu/eli/dir/2022/2555>

[3] Negli anni OAD ha cercato di migliorare la classificazione delle tipologie di attacco e le conseguenti domande nel questionario, ma mantenendo una continuità logica per poter confrontare almeno i dati più significativi ed importanti nell'intero arco temporale di indagine dell'Osservatorio.

[4] DESI, Digital Economy and Society Index, è un indice composito che sintetizza vari rilevanti indicatori sulle prestazioni digitali in Europa e traccia l'evoluzione dei vari membri EU nella competitività digitale.

Si veda <https://digital-strategy.ec.europa.eu/it/policies/desi>



Articolo a cura di **Marco Rodolfo Alessandro Bozzetti**

Profilo Autore

Marco Rodolfo Alessandro Bozzetti



È attualmente Presidente di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, Capitolo Italiano della mondiale ISSA, nel Consiglio Direttivo e Tesoriere di FIDAInform, socio e revisore dei conti del ClubTI di Milano, socio AICA. Dal 2023 partecipa come esperto per AIPSI e Malabo all'iniziativa europea ESSA (<https://www.softwareskills.eu/>) sulle competenze per lo sviluppo di software.

È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". È Commissario d'Esame in AICA per le certificazioni eCFPlus (EN 16234-UNI 11506).

Ha pubblicato circa 300 articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, le normative, gli scenari e gli impatti dell'ICT.

Altri Articoli

This author does not have any more posts.

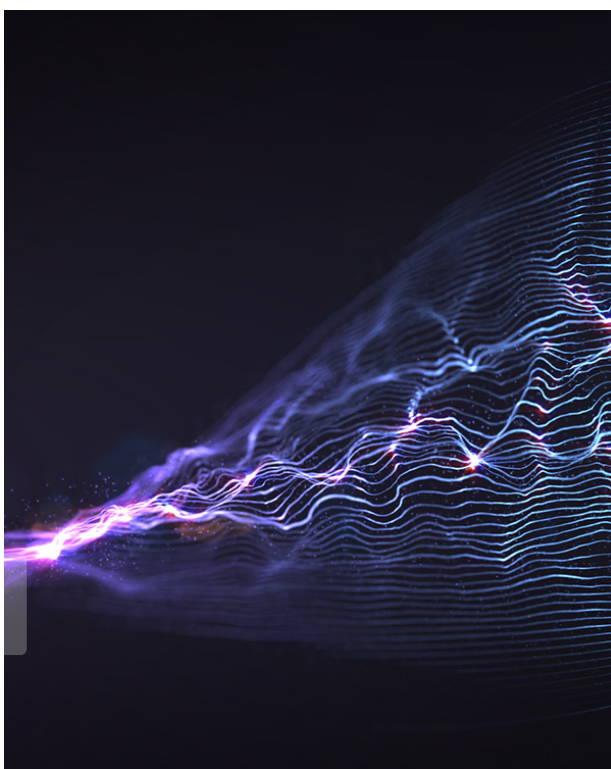
Condividi sui Social Network:

[#AIPSI](#)[#Attacchi Digitali](#)[#cybersecurity](#)[#Osservatorio Attacchi Digitali in Italia](#)

[← PRECEDENTE](#)

Regolamento UE sulla cybersecurity: un nuovo step nella strategia per la sicurezza dello spazio digitale comunitario

Articoli simili



Proteggere le aziende dagli attacchi DDoS

A cura di: Redazione

🕒 Pubblicato il 21 Gennaio 2016

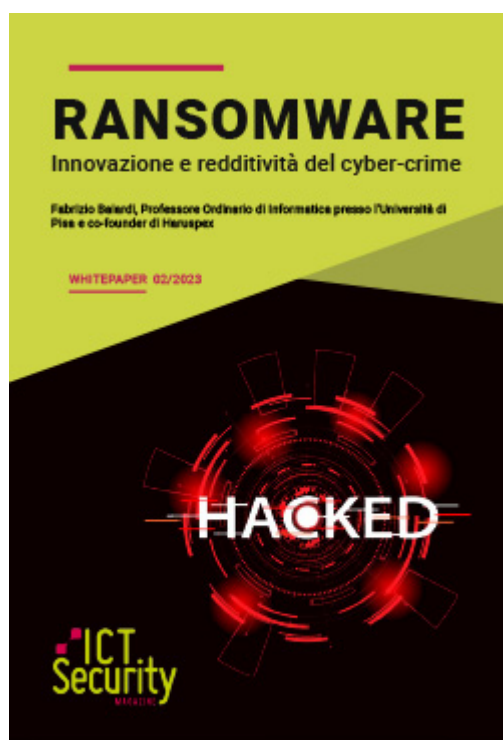


L'Internet of Things fra sicurezza informatica e misure di prevenzione

A cura di: Fabrizio Corona

🕒 Pubblicato il 29 Maggio 2017



[DOWNLOAD GRATUITO](#)

ISCRIVITI ALLA NEWSLETTER

Una volta al mese riceverai gratuitamente la rassegna dei migliori articoli di
ICT Security Magazine

[Iscriviti Ora](#)





[DOWNLOAD GRATUITO](#)

Visualizza il Mar

Manuali Gratis per Aut
Elettrodomestici e Altri

ARGOMENTI

7Layers AI attacchi informatici Blockchain ChatGPT cloud security Crittografia cyber attacchi Cyber Attack Cyber

Crime cybercrime cyber defence cyber intelligence Cyber Risk **Cyber Security**

cybersecurity Cybersicurezza Cyber Threat Intelligence Data Protection data security Digital

Forensics Digitalizzazione GDPR ICT security Incident Response industria 4.0 information security infrastrutture

critiche Intelligenza Artificiale IoT Security Machine Learning Malware Netskope OT Cybersecurity OT security

phishing Privacy ransomware sanità Sicurezza sicurezza informatica SIEM Synopsys Vulnerabilità Zero-

Trust



La Prima Rivista Italiana Dedicata alla Sicurezza Informatica Scarica l'ebook c

ICT SECURITY

MAGAZINE TQSA Srl

ICT Security Magazine 1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.



Segreteria: Humana SRL
C.F e P.IVA: 13642431004
redazione@ictsecuritymagazine.com

ARGOMENTI

7Layers AI attacchi informatici
Blockchain ChatGPT cloud security
Crittografia cyber attacchi Cyber
Attack Cyber Crime
cybercrime cyber defence
cyber intelligence Cyber Risk

Cyber Security cybersecurity

Cybersicurezza Cyber Threat
Intelligence Data Protection
data security Digital Forensics
Digitalizzazione GDPR ICT security
Incident Response industria 4.0
information security infrastrutture
critiche Intelligenza Artificiale
IoT Security Machine Learning
Malware Netskope OT Cybersecurity
OT security phishing Privacy
ransomware sanità Sicurezza
sicurezza informatica SIEM
Synopsys Vulnerabilità Zero-Trust

I NOSTRI SITI:



