Indagine OAD 2021 sugli attacchi digitali in Italia

L'anticipazione dei risultati dell'indagine che da 14 anni fotografa, con l'aiuto della Polizia Postale e delle Comunicazioni, lo scenario degli attacchi informatici nel nostro Paese ad aziende ed enti pubblici

di Marco R. A. Bozzetti,
Presidente AIPSI

Dal 2007 AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, realizza l'indagine indipendente OAD (Osservatorio Attacchi Digitali) per analizzare il fenomeno degli attacchi digitali ai sistemi informatici di aziende ed enti pubblici in Italia.

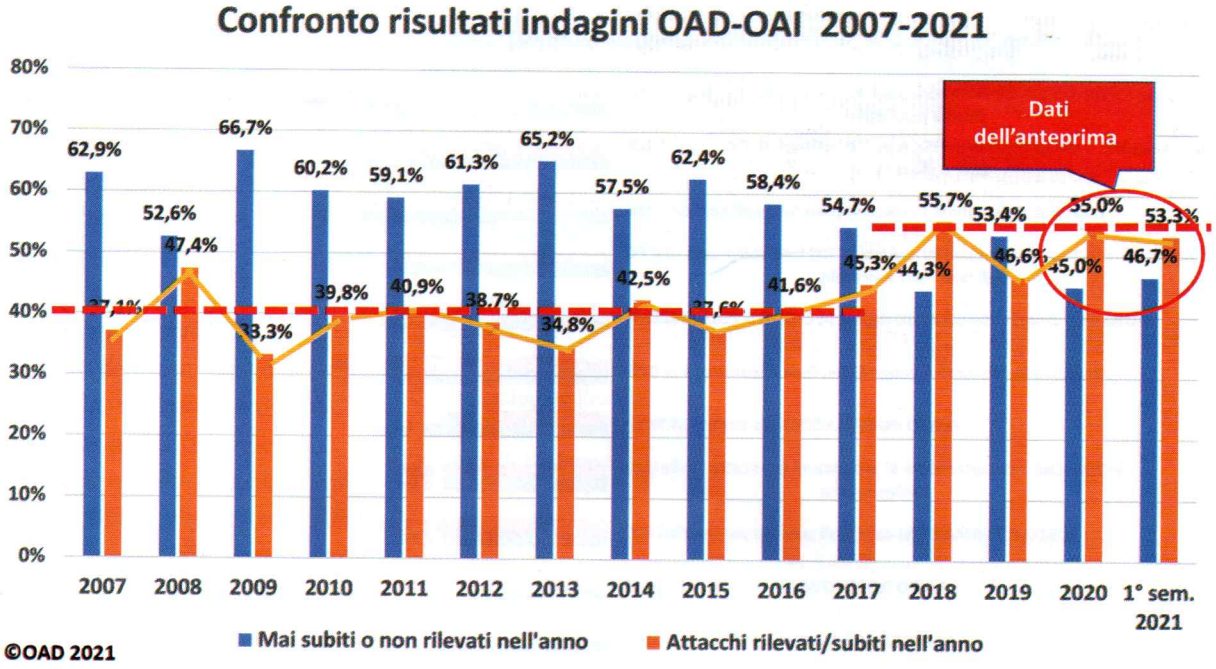
L'indagine, unica nel suo genere, si focalizza sullo scenario locale italiano fornendo indicazioni sulla tipologia e l'ampiezza del fenomeno utili per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione.

La Polizia Postale e delle Telecomunicazioni da anni collabora con l'indagine OAD fornendo suoi dati sugli attacchi alle infrastrutture critiche, sulle frodi finanziarie online e sul cyber terrorismo. Nel 2021, inoltre, OAD è stata includa tra i progetti di Repubblica Digitale per la sua rilevanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity.

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

AIPSI (https://www.aipsi.org) è la libera associazione no-profit, che raduna a livello individuale chi è interessato professionalmente alla sicurezza informatica, in qualsiasi ruolo e modalità. AIPSI è il capitolo italiano di ISSA, Information System Security Association (https://www.issa.org/), la più grande organizzazione analoga a livello mondiale, che conta complessivamente oltre 13mila soci. Il Socio AIPSI è contemporaneamente anche Socio ISSA.

Gli obiettivi principali di AIPSI sono di aiutare i propri soci nella crescita professionale e delle competenze e di diffondere la cultura della sicurezza digitale.



L'indagine 2021 è in fase di completamento e ve ne anticipiamo i risultati che potrebbero subire lievi variazioni. Il rapporto OAD 2021 definitivo (così come tutti quelli realizzati da AIPSI dal 2007 a oggi) può essere scaricato gratuitamente dal sito https://www.oadweb.it.

Il trend degli attacchi digitali in Italia

La quasi totalità dei rispondenti all'indagine 2021 appartiene ad aziende private e, di queste, quasi l'80% sono Piccole Medie Imprese con meno di 250 dipendenti. Un dato che rispecchia i più recenti dati Istat (2019) secondo cui, in Italia, su 4milioni e 304mila imprese, il 64,03% è senza dipendenti, il 31,65% ne ha meno di 10, il 4,22% tra 10 e 250 e solo lo 0,1% ha più 250 dipendenti. Per le PA la situazione è analoga: poche le PA di grandi dimensioni, come i Ministeri ed i grandi Comuni, e moltissime le piccole e piccolissime organizzazioni.

Un primo dato interessante è l'andamento del fenomeno attacchi digitali ad aziende ed enti pubblici in Italia dal 2007 al 2021, con un trend a onda, in una costante rincorsa tra guardie e ladri digitali a migliorare gli attacchi e potenziare le misure di prevenzione e protezione.

Nel 2018, per la prima volta, la percentuale di aziende che ha dichiarato di aver subito un attacco ha superato quella di chi lo ha negato. Negli ultimi 18 mesi la percentuale si assesta a circa il 55%.

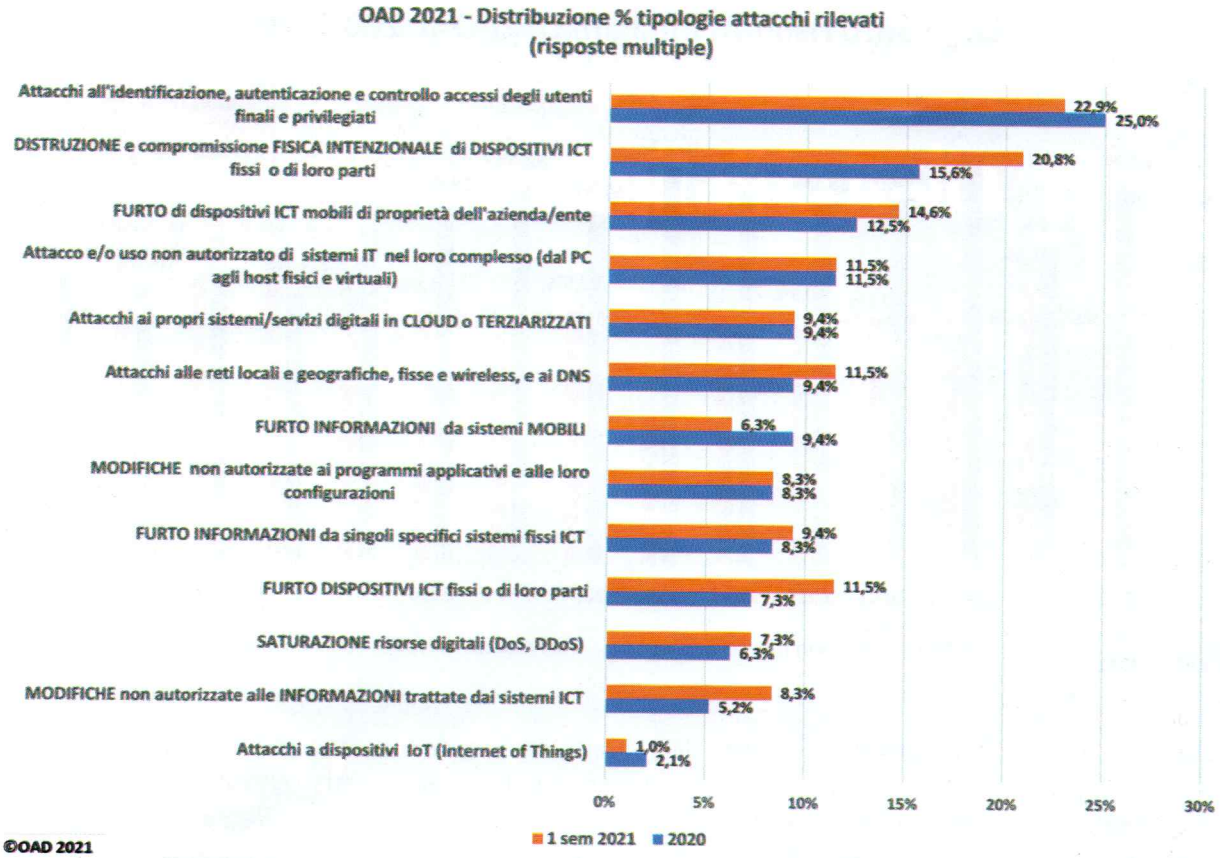
Si tratta di una percentuale che può sembrare bassa ma che va interpretata considerando il numero prevalente di piccole e piccolissime aziende ed enti che sono stati interpellati. Le realtà piccole, infatti, non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per gli attacchi mirati, potendo più facilmente essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware. Questo aspetto trova conferma nell'analisi della correlazione tra attacchi rilevati e dimensioni aziendali che evidenzia una crescita molto significativa di dichiarazioni di attacchi subiti da parte delle aziende più grandi.

Tipologie e tecniche di attacco

L'indagine ha considerato 14 tipologie di attacco suddivise in base all'obiettivo: il sistema digitale fisico, il suo controllo degli accessi, le sue applicazioni, la sua rete di comunicazione, i dati trattati e così via.

Al primo posto come tipologia percentualmente più diffusa si conferma quella degli attacchi ai sistemi di identificazione, autenticazione, autorizzazione: in pratica ai sistemi di controllo degli accessi ai sistemi digitali. Un primato assai critico, dato che si tratta dell'elemento chiave per sottrarre e usare in maniera dolosa l'identità di digitale di altri utenti, sovente quelli privilegiati.

Al secondo posto la distruzione fisica di

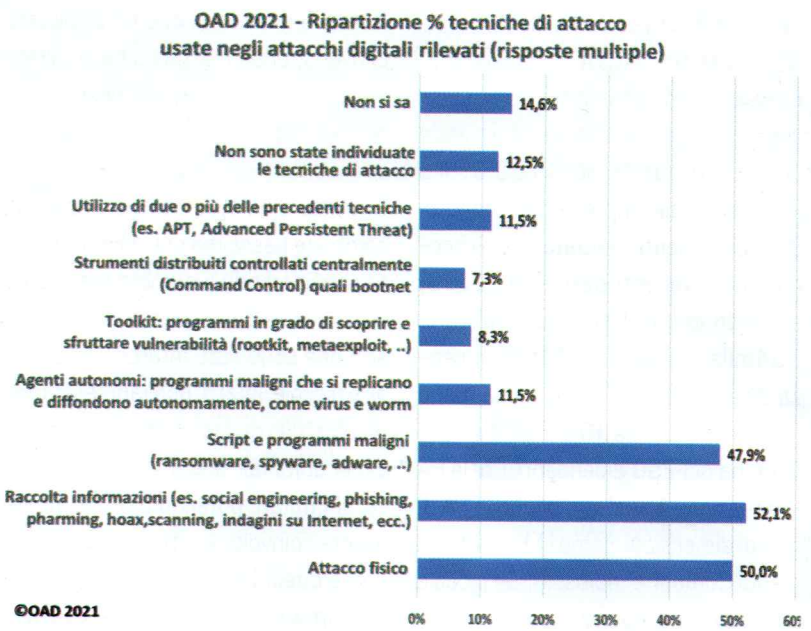


dispositivi ICT o di loro parti e al terzo il furto di dispositivi mobili: quest'ultimo un attacco da tempo diffuso e in certi anni posizionato in cima alle classifiche di OAD, alla luce della semplicità di attuazione e del valore del dispositivo, in particolare per gli smartphone.
Tra tecniche utilizzate negli attacchi al primo posto si posiziona il social engineering utilizzato per raccogliere informazioni a cui seguono, a breve distanza percentuale, gli attacchi fisici e l'uso di script e malware.

I dati dalla Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni da anni collabora con AIPSI fornendo significativi dati sulle azioni svolte in Italia sul fronte del contrasto agli attacchi digitali e ai crimini informatici, con particolare riferimento alle infrastrutture critiche, al crimine digitale finanziario e al cyber terrorismo.

Il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) è una



struttura della Polizia Postale e delle Comunicazioni incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici di matrice comune, organizzata o terroristica, che hanno come obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

I dati relativi al primo quadrimestre del 2021 evidenziano il trend di crescita degli allarmi emanati e diramati che prosegue dal 2016.

Differente è il dato del numero di attacchi rilevati alle infrastrutture critiche, che oscilla periodicamente negli ultimi anni tra incrementi e decrementi. Oltre al ben noto inseguimento tra guardie e ladri cibernetici, ormai giocato a livello mondiale, può influire su questi dati il riposizionamento di NIS 2 (la Direttiva europea che punta a omogeneizzare gli obblighi in termini di cybersecurity per le infrastrutture critiche), con l'estensione anche del tipo di servizi essenziali e del perimetro di cybersecurity nazionale.

Un dato evidente è la forte disparità tra il numero di indagini avviate rispetto agli attacchi rilevati e, ancora più basso, il numero di persone denunciate, indagate e alla fine arrestate. Il problema di fondo è che, a fronte di centinaia di attacchi rilevati, alla fine gli arrestati si contano su una mano: il cyber crime rimane di fatto quasi impunito, nonostante l'Italia abbia adottato da anni una precisa e severa legislazione (anche in ambito penale) relativa al crimine informatico e vi sia una forza specifica di Polizia, la Polizia Postale, operante sul territorio e con il supporto di unità specializzate dell'Arma dei Carabinieri e della Finanza.

Gli attacchi digitali agli ambienti e alle transazioni finanziarie sono prevalentemente finalizzati a ottenere un illecito guadagno economico, per cui ogni transazione economica rappresenta un potenziale target. Questo tipo di crimine informatico include anche attacchi indirizzati alle piattaforme di e-commerce, ivi inclusi i relativi pagamenti online.

La buona notizia è che le transazioni finanziarie bloccate dalla Polizia Postale nell'ultimo periodo sono in aumento: se il trend dei primi 4 mesi del 2021 si confermasse arriverebbero al doppio rispetto al 2020. In aumento anche le somme recuperate, a conferma del continuo miglioramento delle capacità di contrasto da parte della Polizia Postale.

Il numero di siti Web controllati dalla Polizia Postale che, insieme ad alcune social net, sono alla base e contribuiscono al proselitismo, alla preparazione e al coordinamento di attacchi terroristici, negli anni è aumentato leggermente, e si mantiene nell'ordine di 36mila. Queste cifre forniscono una chiara indicazione della vastità e complessità del problema che quotidianamente occorre contrastare. ❄

	gen. - apr. 2021	2020	2019	2018	2017	2016
Attacchi rilevati	282	509	1.181	459	1.032	844
Allarmi diramati	**24.824**	**83.416**	**82.484**	**80.777**	**31.254**	**6.721**
Indagini avviate	34	103	155	74	72	70
Persone arrestate	**0**	**n.d.**	**3**	**1**	**3**	**3**
Persone denunciate/ indagate	0	105	117	14	1.316	1.226
Perquisizioni	**n.d.**	**n.d.**	**n.d.**	**n.d.**	**73**	**58**
Richiesta di coop. internazionale Rete 24/7 High Tech Crime G8 (Conv. di Budapest)	17	69	79	108	83	85

Attività svolte dal C.N.A.I.P.I.C. nel periodo 2016-2021 (I° quadrimestre) sulle infrastrutture critiche italiane (Fonte Polizia Postale e delle Comunicazioni)

	gen. - apr. 2021	2020	2019	2018	2017	2016
Transazioni fraudolente bloccate	€ 20.200.000	€ 33.186.674	€ 21.333.990	€ 38.400.000	€ 20.839.576	€ 16.050.813
Somme recuperate	**24.824 €**	**83.416 €**	**82.484 €**	**80.777 €**	**31.254 €**	**n.d.**
Percentuale di recupero di somme frodate	43,07%	60,40%	84,37%	23,44%	4,14%	n.d.

Attività della Polizia Postale in contrasto al Financial Cyber Crime (Fonte: Polizia Postale e delle Comunicazioni)