Agosto 2025

Report di mercato

Il rapporto Ransomware Insights 2025

Analisi dell'esperienza e dell'impatto del ransomware sulle organizzazioni a livello globale

Barracuda®
Your business, secured.

Sommario

Introduzione 3

Risultati chiave 5

Il ransomware colpisce più della metà delle organizzazioni 6

Le vittime di ransomware hanno un profilo diverso per gli strumenti di sicurezza e le priorità 6

Le bande di ransomware hanno una possibilità su tre di ottenere un pagamento 8

La crittografia dei dati è ora solo una parte di un attacco ransomware 8

Le vittime di ransomware perdono clienti e nuove opportunità commerciali 10

Conclusione 11

Introduzione

Il ransomware è una minaccia diffusa e in continua evoluzione, alimentata da kit ransomware-as-a-service che consentono a un numero sempre maggiore di criminali informatici di lanciare attacchi. Gli incidenti di ransomware possono danneggiare la reputazione del marchio e paralizzare le operazioni quotidiane, causando interruzioni, perdita di dati, fiducia dei clienti e altro ancora. Ogni organizzazione è un potenziale bersaglio.

Questo rapporto esplora l'esperienza e l'impatto degli attacchi ransomware riusciti sulle organizzazioni di tutto il mondo negli ultimi 12 mesi. Si basa sui risultati di un sondaggio internazionale su 2.000 decisori IT e di sicurezza condotto da Barracuda e Vanson Bourne.

I risultati possono essere raggruppati in tre temi generali:

- **Le vittime di ransomware hanno maggiori probabilità di avere una sicurezza frammentata,** con troppi strumenti di sicurezza disconnessi e una copertura insufficiente nelle aree chiave della sicurezza.
- **Gli attacchi ransomware sono multidimensionali.** Non riguardano più solo la crittografia dei dati, ma ora comportano il furto e l'esposizione dei dati, l'installazione di payload dannosi aggiuntivi e altro ancora.
- **Il raggio di impatto di un attacco ransomware riuscito si allarga,** includendo la perdita di nuove opportunità commerciali e tattiche di pressione per il pagamento che si estendono a dipendenti, partner, clienti e autorità.

Metodologia

Barracuda ha incaricato la società indipendente di ricerche di mercato Vanson Bourne di condurre un sondaggio globale su 2.000 responsabili senior in materia di sicurezza in ruoli IT e aziendali in organizzazioni con un numero di dipendenti compreso tra 50 e 2.000, provenienti da un'ampia gamma di settori negli Stati Uniti, Regno Unito, Francia, DACH (Germania, Austria, Svizzera), Benelux (Belgio, Paesi Bassi, Lussemburgo), i Paesi nordici (Danimarca, Finlandia, Norvegia, Svezia), Australia, India e Giappone. Il lavoro sul campo è stato condotto ad aprile e maggio 2025.

Introduzione

Ci auguriamo che questo rapporto aiuti le organizzazioni di tutte le dimensioni e settori a comprendere la minaccia e l'impatto del ransomware nel 2025 e a identificare e affrontare le aree in cui potrebbero essere potenzialmente a rischio.

Risultati principali

57%

delle organizzazioni ha subito un attacco ransomware riuscito negli ultimi 12 mesi

71%

delle organizzazioni che hanno subito una violazione e-mail sono state colpite anche dal ransomware

32%

ha pagato un riscatto per recuperare i propri dati — il 41% di loro non ha recuperato tutti i dati

65%

di vittime del ransomware ha potuto ripristinare i dati dai backup

24%

delle vittime del ransomware aveva i dati crittografati, mentre il 27% ha subito il furto dei dati e il 29% ha dichiarato che gli attaccanti hanno installato payload aggiuntivi

25%

delle vittime di ransomware ha perso clienti esistenti — la stessa proporzione ha perso nuove opportunità di business

Il ransomware colpisce più della metà delle organizzazioni

Complessivamente, il 57% delle organizzazioni intervistate ha subito un attacco ransomware riuscito negli ultimi 12 mesi.

Una vittima su tre (31%) è stata colpita due o più volte.

La prevalenza di attacchi multipli riusciti suggerisce che le lacune di sicurezza non vengono investigate e risolte in modo completo dopo ogni incidente. In questo rapporto esaminiamo la differenza tra le organizzazioni colpite una volta e quelle colpite più volte per vedere cosa si può imparare dai dati e come le organizzazioni possono utilizzarli per migliorare il loro livello di sicurezza.

I settori più colpiti nel nostro sondaggio includevano l'assistenza sanitaria (con il 67% delle organizzazioni colpite), il governo locale (65%) e il commercio al dettaglio (61%). Secondo i dati, l'industria manifatturiera è stata la meno colpita, con poco meno della metà (46%) degli intervistati che ha riportato un attacco riuscito.

Le dimensioni non sembrano essere un fattore quando si tratta di ransomware, e i risultati rimangono coerenti in tutte le fasce di dimensioni delle aziende intervistate, da 50 a 2.000 dipendenti.

Il 71% delle organizzazioni che avevano subito una violazione delle e-mail sono state colpite anche dal ransomware: questo evidenzia il legame tra i due tipi di attacco.

Le vittime di ransomware hanno un profilo diverso per gli strumenti di sicurezza e le priorità

Crescita incontrollata degli strumenti di sicurezza e rischio di ransomware

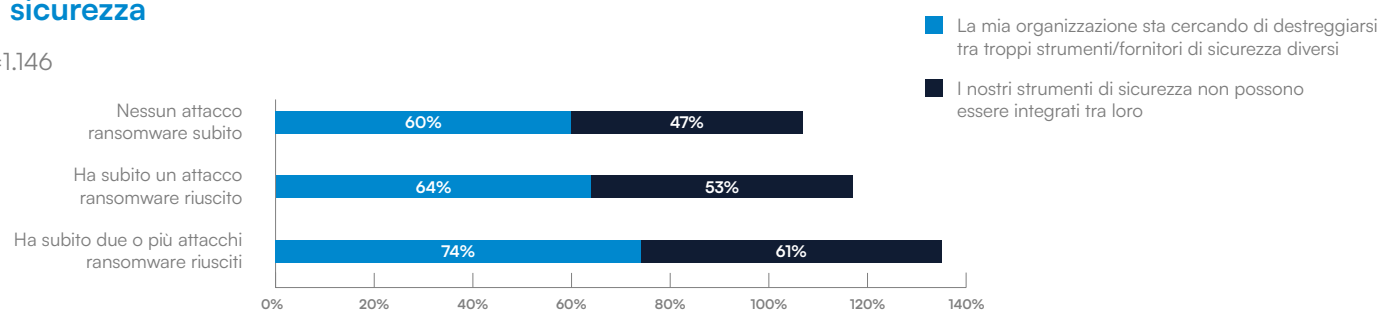
Il sondaggio mostra che un eccesso di strumenti di sicurezza, noto con l'espressione inglese "security sprawl", accompagnati da una mancanza di integrazione può aumentare il rischio e creare lacune nella protezione rendendo più difficile per le organizzazioni rilevare e mitigare le minacce attive, incluso il ransomware.

I dati mostrano che la percentuale di organizzazioni colpite dalla crescita incontrollata degli strumenti di sicurezza o dalla mancanza di integrazione aumenta in linea con il loro tasso di attacchi ransomware subiti.

FIGURA 1

Incidenti ransomware e crescita incontrollata degli strumenti di sicurezza

n=1.146



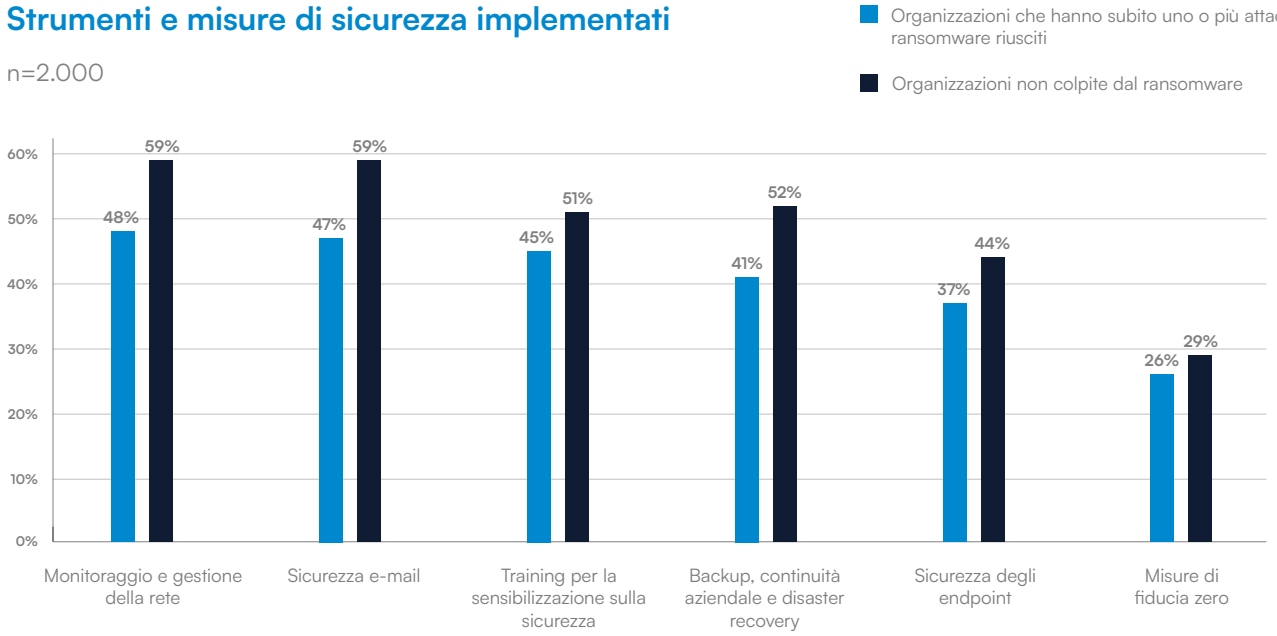
I diversi tipi di strumenti e misure di sicurezza

Secondo gli intervistati, le misure di sicurezza più ampiamente implementate sono la sicurezza e-mail (implementata dal 52%), la sicurezza della rete (52%) e il training per la sensibilizzazione sulla sicurezza (48%). Le organizzazioni che hanno segnalato un incidente di ransomware riuscito hanno meno probabilità di aver implementato una di queste misure.

FIGURA 2

Strumenti e misure di sicurezza implementati

n=2.000



Ad esempio:

- Il 47% delle vittime di ransomware aveva implementato una soluzione di sicurezza email, rispetto al 59% delle non vittime
- Il 48% delle vittime di ransomware disponeva di gestione e monitoraggio della rete, rispetto al 59% delle non vittime
- Il 45% delle vittime di ransomware aveva ricevuto un training per la sensibilizzazione sulla sicurezza, rispetto al 51% delle non vittime
- Il 37% ha implementato la sicurezza degli endpoint, rispetto al 44% delle non vittime

Questi risultati suggeriscono che le vittime del ransomware potrebbero investire poco in aree di sicurezza che potrebbero contribuire a ridurre la loro esposizione al rischio.

Ad esempio, la Sicurezza delle e-mail, della rete e degli endpoint, insieme al training per la sensibilizzazione sulla sicurezza, forniscono una solida difesa contro gli attacchi di phishing e social engineering trasmessi via e-mail progettati per rubare credenziali e consentire agli attaccanti di violare le reti, compromettere i dispositivi e spostarsi lateralmente: tutte tecniche caratteristiche di un attacco ransomware.

I criminali che usano il ransomware hanno una probabilità su tre di ricevere un pagamento

Il 32% delle vittime di ransomware ha pagato un riscatto per recuperare o ripristinare i dati.

I risultati mostrano una correlazione tra la propensione di un'organizzazione a pagare un riscatto e il numero di volte in cui viene colpita dal ransomware.

Le organizzazioni che hanno subito un solo attacco ransomware riuscito avevano una probabilità leggermente inferiore di pagare il riscatto, con il 29% che lo ha fatto, mentre tra le persone colpite due o più volte, il 37% ha pagato il riscatto per riavere i propri dati.

Questi dati sono rimasti pressoché invariati rispetto all'ultima indagine condotta due anni fa. Nel 2023, i risultati hanno mostrato che il 31% delle persone colpite una volta e il 38% delle persone colpite due o più volte hanno pagato un riscatto per recuperare i dati.

Una possibile spiegazione del collegamento tra gli attacchi multipli e i pagamenti di ransomware è che una volta dimostrato che un'organizzazione è disposta a pagare, altri attaccanti prenderanno di mira la stessa vittima, o lo stesso attaccante potrebbe tornare più di una volta.

La buona notizia è che la maggior parte (65%) delle vittime di ransomware è stata in grado di ripristinare i propri dati utilizzando i backup.

A riprova del fatto che pagare il riscatto non è una soluzione efficace, il 41% di coloro che hanno pagato (13% in totale) non hanno recuperato tutti i dati o non ne hanno recuperato addirittura nessuno.

La crittografia dei dati è ora solo una parte di un attacco ransomware

A parte l'onere finanziario del pagamento di un riscatto, la ricerca mostra che l'impatto commerciale, operativo e persino emotivo di un attacco ransomware riuscito è considerevole.

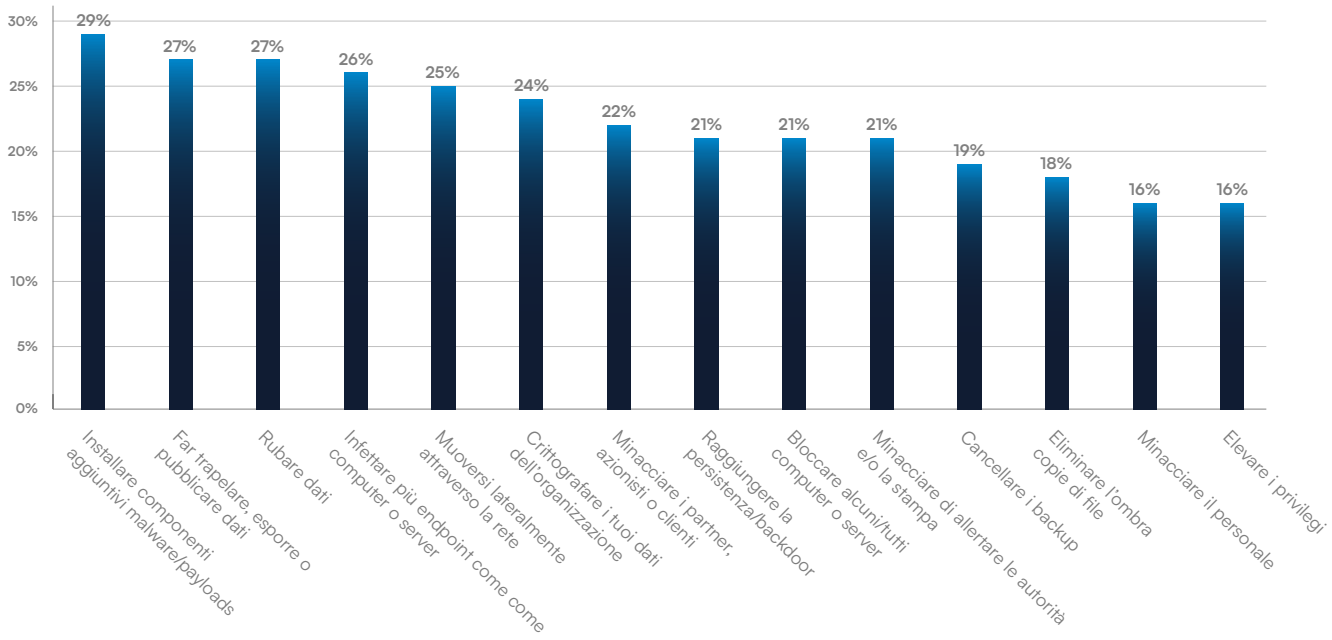
Nella maggior parte degli incidenti di ransomware, la crittografia dei dati e il blocco dei sistemi e dei computer rappresentano generalmente la fase finale. Questa è la parte più visibile dell'attacco e quindi la più probabile a rivelare la presenza di intrusi al team di sicurezza e a comportare il contenimento e la rimozione della minaccia.

I risultati della ricerca sottolineano l'ampiezza delle attività che si svolgono sotto il radar prima dell'esecuzione del ransomware, per consentire l'attacco o potenzialmente aprire la strada ad altre attività.

FIGURA 3

Attività intraprese dalle bande di ransomware durante l'incidente più significativo

n=1.146



Circa un quarto degli incidenti di ransomware riportati dagli intervistati ha coinvolto la crittografia dei dati (24%), il blocco degli endpoint (21%) e il furto di dati (27%).

Gli attacchi comprendono anche il movimento laterale attraverso la rete (25%), l'infezione di più endpoint come computer o server (26%), l'installazione di payload dannosi aggiuntivi (29%), l'elevazione dei privilegi (16%) e l'integrazione di backdoor e altri meccanismi di persistenza (21%).

Inoltre, per rendere più difficile per le vittime ripristinare i propri dati senza pagare, circa un attaccante su cinque ha eseguito l'accesso e cancellato i backup ed eliminato le copie shadow dei file (entrambe le operazioni sono state riscontrate dal 19% delle vittime).

I risultati mostrano anche che una volta eseguito il ransomware e inviata la richiesta di pagamento, gli attaccanti iniziano a esercitare pressioni sulla vittima attraverso tattiche psicologiche. Queste includono la minaccia a partner, azionisti o clienti (esperienza del 22%), la minaccia di allertare la stampa o le autorità (21%) e persino la minaccia al personale (16%).

Nel 27% degli incidenti di ransomware riusciti, gli attaccanti hanno continuato a divulgare, esporre o pubblicare i dati rubati.

Le vittime di ransomware perdono clienti e nuove opportunità commerciali

Una volta che le acque si sono calmate riguardo all'attacco vero e proprio, le vittime si trovano ad affrontare ripercussioni operative e commerciali.

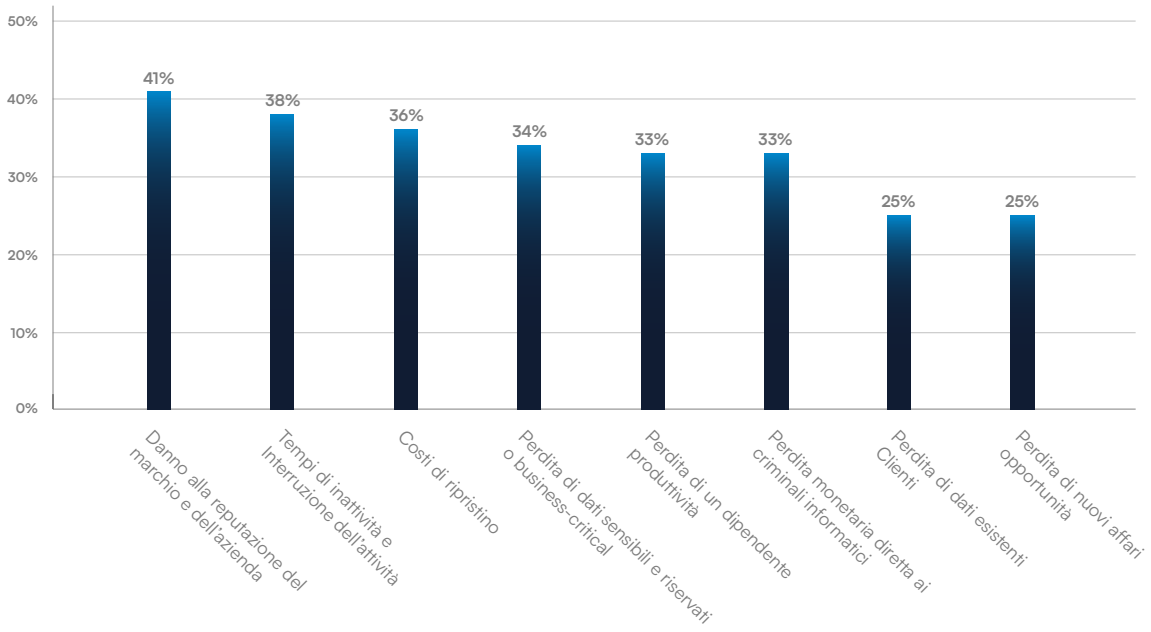
L'impatto principale citato dalle vittime del ransomware è stato il danneggiamento del marchio e della reputazione (che ha influito sul 41%). Seguono i tempi di inattività (38%) e i costi di ripristino (36%). Un terzo (34%) ha ammesso di aver perso dati sensibili.

Una vittima di ransomware su quattro ha affrontato l'impatto aziendale a lungo termine della perdita di clienti esistenti e di nuove opportunità di business (entrambi 25%).

FIGURA 4

L'impatto dell'attacco ransomware più significativo degli ultimi 12 mesi

n=1.146



Conclusione

Per essere resilienti al ransomware, le organizzazioni necessitano di una sicurezza integrata e multilivello che protegga dalle minacce informatiche la loro superficie di attacco in continua espansione.

I seguenti passaggi pratici possono aiutare:

- **Assicurarsi che i dati vengano sottoposti a backup regolari e sicuri** e che vengano mantenuti offline. Eseguire dei test per assicurarsi di poter ripristinare efficacemente i dati.
- **Implementare l'autenticazione multifattoriale e applicare il principio del privilegio minimo** per limitare l'accesso alle risorse e alle applicazioni aziendali. Questo impedisce agli attaccanti di prendere di mira dati e sistemi di alto valore anche con credenziali rubate.
- **Mantenere il software aggiornato** con le ultime patch di sicurezza per colmare le lacune di sicurezza.
- **Fornire regolarmente ai dipendenti corsi di formazione** sulla consapevolezza della sicurezza informatica, concentrandosi sulle ultime tattiche di phishing e ransomware.
- **Segmentare la rete,** isolando i sistemi critici per prevenire il movimento laterale da parte degli attaccanti.
- **Controllare tutte le configurazioni,** incluse quelle nel cloud. Le configurazioni errate sono un fattore chiave per le violazioni della sicurezza.
- **Installare una soluzione di sicurezza email affidabile.** L'e-mail rimane un punto di ingresso primario per il ransomware, e una protezione avanzata basata sull'IA può rilevare payload dannosi e riconoscere tattiche avanzate di social engineering progettate per aggirare la sicurezza.
- **Proteggere le applicazioni web come i servizi di condivisione file,** i moduli web e i siti di e-commerce. Le applicazioni sono spesso prese di mira tramite l'interfaccia utente o un'interfaccia API.
- **Avere un piano di incident response e provarlo regolarmente.**
- **Prendi in considerazione la collaborazione con esperti esterni**, inclusi i provider di servizi gestiti e i fornitori di sicurezza, per un ottenere un ulteriore supporto. Questi partner possono aiutarti nell'implementazione di piattaforme e soluzioni di sicurezza integrate avanzate per rilevare, bloccare e rispondere alle minacce attive 24/7, contenendo e neutralizzando gli incidenti prima che possano causare gravi danni.

Informazioni su Barracuda

Barracuda è un'azienda leader globale nel settore della sicurezza informatica che offre una protezione completa contro le minacce complesse per le aziende di qualsiasi dimensione. La nostra piattaforma basata sull'IA protegge e-mail, dati, applicazioni e reti con soluzioni innovative, XDR gestito e una dashboard centralizzata per ottimizzare la protezione e rafforzare la resilienza informatica. Scelto da centinaia di migliaia di professionisti IT e provider di servizi gestiti in tutto il mondo, Barracuda offre difese potenti e facili da acquistare, implementare e utilizzare.

Barracuda Networks, Barracuda, BarracudaONE e il logo Barracuda Networks sono marchi registrati o marchi di Barracuda Networks, Inc. negli Stati Uniti e in altri Paesi.

Informazioni su Vanson Bourne

Vanson Bourne è uno specialista indipendente nella ricerca di mercato nel settore tecnologico. La sua reputazione per un'analisi solida e credibile basata sulla ricerca si fonda su principi di ricerca rigorosi e sulla capacità di raccogliere le opinioni dei decisori senior in tutte le funzioni tecniche e aziendali, in tutti i settori e in tutti i principali mercati. Per ulteriori informazioni, visita il sito vansonbourne.com.