M-TRENDS 2022

REPORT SPECIALE MANDIANT

SINTESI GENERALE

I recenti eventi informatici ci hanno ricordato brutalmente che il nostro lavoro di difensori non finisce mai. Vulnerabilità critiche, come ad esempio "Log4Shell", mettono in evidenza i pericoli dell'ignoto e la complessità dell'applicazione delle patch. La supply chain è sempre un obiettivo allettante, visto che fornisce un potenziale punto di ingresso a sistemi di più fornitori. Inoltre, dobbiamo rimanere vigili sulla protezione dei nostri sistemi di controllo industriale, soprattutto perché 1 su 7 attacchi di estorsione di vario tipo diffondono informazioni critiche sulla tecnologia operativa.

Gli analisti Mandiant si impegnano ogni giorno in prima linea, indagando e analizzando gli attacchi e le minacce più recenti per capire come rispondere al meglio e mitigarne l'impatto. Tutto ciò che impariamo viene trasmesso ai nostri clienti attraverso i nostri diversi servizi, che offrono loro un vantaggio indispensabile in un panorama di minacce in costante evoluzione.

Ogni anno il report *M-Trends* fornisce alcune di queste informazioni critiche alla comunità della sicurezza a livello più ampio.*M-Trends 2022* continua il lavoro degli anni passati, offrendo informazioni dettagliate sul panorama informatico in evoluzione, sulle raccomandazioni di mitigazione e su un'ampia varietà di metriche relative agli incidenti correlati alla sicurezza.

Iniziamo con una vittoria per i difensori: il tempo di attesa mediano globale ha continuato a scendere nel corso del 2021. Nelle intrusioni analizzate tra il 1º ottobre 2020 e il 31 dicembre 2021, il tempo mediano tra la compromissione e il rilevamento è stato di 21 giorni (rispetto ai 24 giorni del 2020). Sebbene questa tendenza possa indicare una migliore visibilità e risposta, in realtà è stata la pervasività del ransomware a contribuire ad abbassare questo numero.

Ransomware ed estorsione di varia forma continuano ad essere preoccupanti. Registriamo un aumento del targeting dell'infrastruttura di virtualizzazione e offriamo mitigazioni. Forniamo inoltre indicazioni sulla preparazione alla gestione del ransomware (tramite il red team) e sulle operazioni di ripristino.

Altri argomenti trattati nel report *M-Trends 2022* includono:

In base ai numeri Il tempo di attesa mediano globale per le intrusioni identificate da terze parti esterne e comunicate alle vittime è sceso a 28 giorni rispetto ai 73 del 2020, un miglioramento eccezionale. La notizia meno positiva è che, nei casi in cui è stato identificato il vettore di infezione iniziale, la compromissione della supply chain rappresentava il 17% delle intrusioni nel 2021 rispetto a meno dell'1% nel 2020. Altre metriche di firma includono il rilevamento in base alla fonte, il targeting del settore, i gruppi di aggressori, il malware e le tecniche degli autori dell'attacco.

Gruppi di aggressori classificati di recente Un'analisi dettagliata di due gruppi di aggressori con motivazione finanziaria classificati nel 2021: FIN12 e FIN13. Segnaliamo anche due gruppi non classificati degni di nota: UNC2891 e UNC1151.

Caso di studio Microsoft Exchange Le nostre osservazioni in risposta a oltre 20 incidenti che implicano lo sfruttamento dei server Microsoft Exchange in loco. In una testimonianza di indagini e analisi dedicate, l'impiego di coniatori di criptovalute da parte di un gruppo di minacce con motivazione finanziaria ha portato alla scoperta di due attori stato-nazione negli stessi ambienti.

Operazioni informatiche in Cina Vengono esaminati il riallineamento e la riorganizzazione della Cina, vengono esplorate le attività di spionaggio e vengono messi in evidenza attori come APT10 e APT41.

Mitigazioni delle configurazioni errate Abbiamo osservato varie compromissioni a causa di errori di configurazione quando viene utilizzato Active Directory in loco con Azure Active Directory per ottenere un'unica soluzione di identità integrata.

M-Trends 2022 sfrutta la nostra trasparenza per continuare a fornire conoscenze critiche a coloro che hanno il compito di difendere le organizzazioni. Le informazioni contenute in questo report sono state trattate in modo tale da proteggere l'identità delle vittime e i rispettivi dati.

IN BASE AI NUMERI

DATI DERIVANTI DALLE INDAGINI MANDIANT

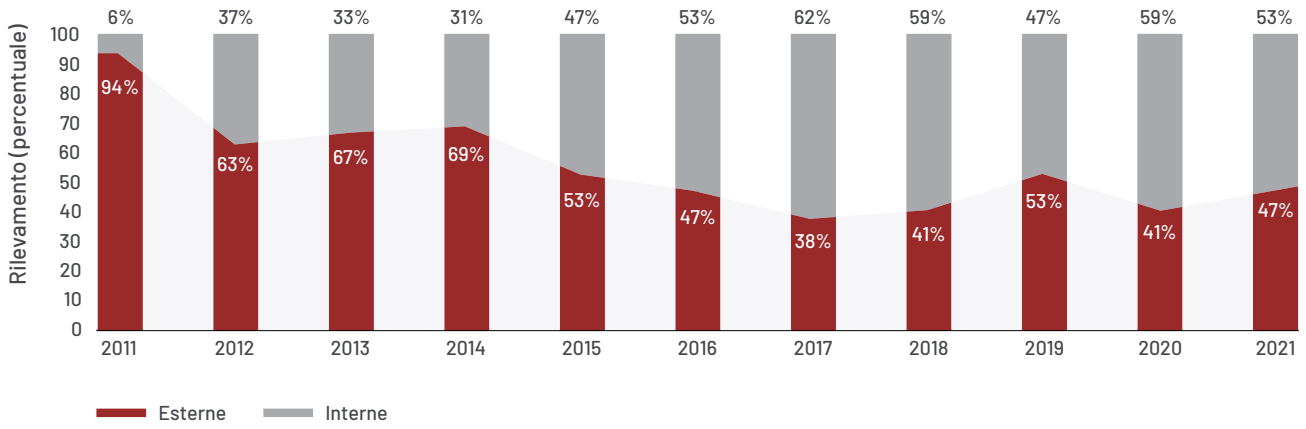
Le metriche indicate nel report *M-Trends 2022* si basano sulle indagini condotte da Mandiant in merito ad attività di attacchi mirati, eseguiti tra il 1° ottobre 2020 e il 31 dicembre 2021.

Questa edizione di *M-Trends* copre un periodo di 15 mesi rispetto a un periodo di 12 mesi delle edizioni precedenti.

Rilevamento per fonte

In generale, nel 2021 è stato registrato un aumento della notifica esterna delle intrusioni rispetto al 2020. Tuttavia, la conoscenza della maggior parte delle intrusioni continua ad essere ottenuta attraverso rilevamenti interni. La percentuale di intrusioni rilevate internamente ha mantenuto una graduale tendenza al rialzo con fluttuazioni moderate negli ultimi sei anni.

Rilevamento per fonte, 2011-2021

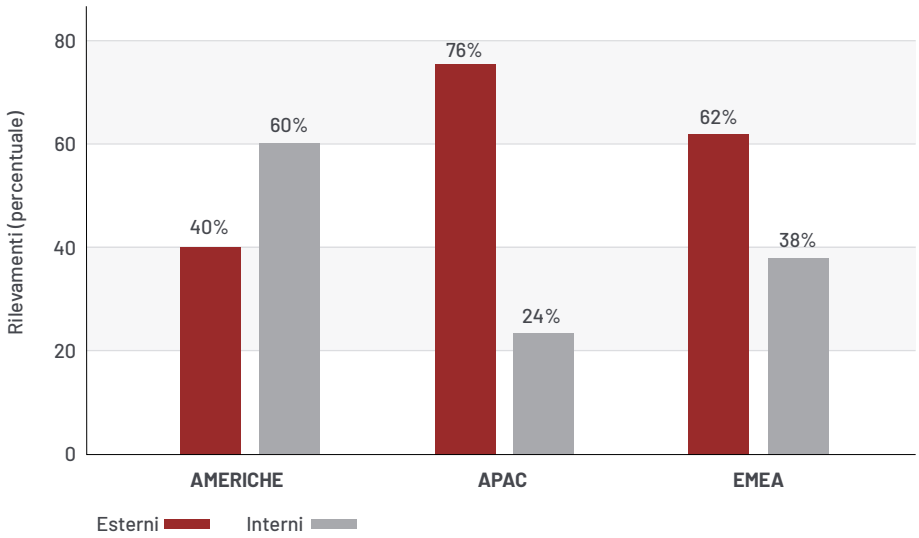


Nelle aree APAC ed EMEA, la maggior parte delle intrusioni del 2021 è stata identificata esternamente, un'inversione di tendenza rispetto a quanto osservato nel 2020. Il rilevamento in base alla fonte per le Americhe si è mantenuto coerente, mostrando come la maggior parte delle intrusioni continui ad essere rilevata internamente.

Il rilevamento interno si verifica quando un'organizzazione scopre autonomamente di essere stata compromessa.

La notifica esterna si verifica quando un'entità esterna comunica a un'organizzazione l'avvenuta compromissione. Questo include quando un'organizzazione compromessa viene avvisata per la prima volta di un incidente da parte di un autore di un attacco tramite un messaggio di estorsione.

Rilevamento per fonte per area, 2021

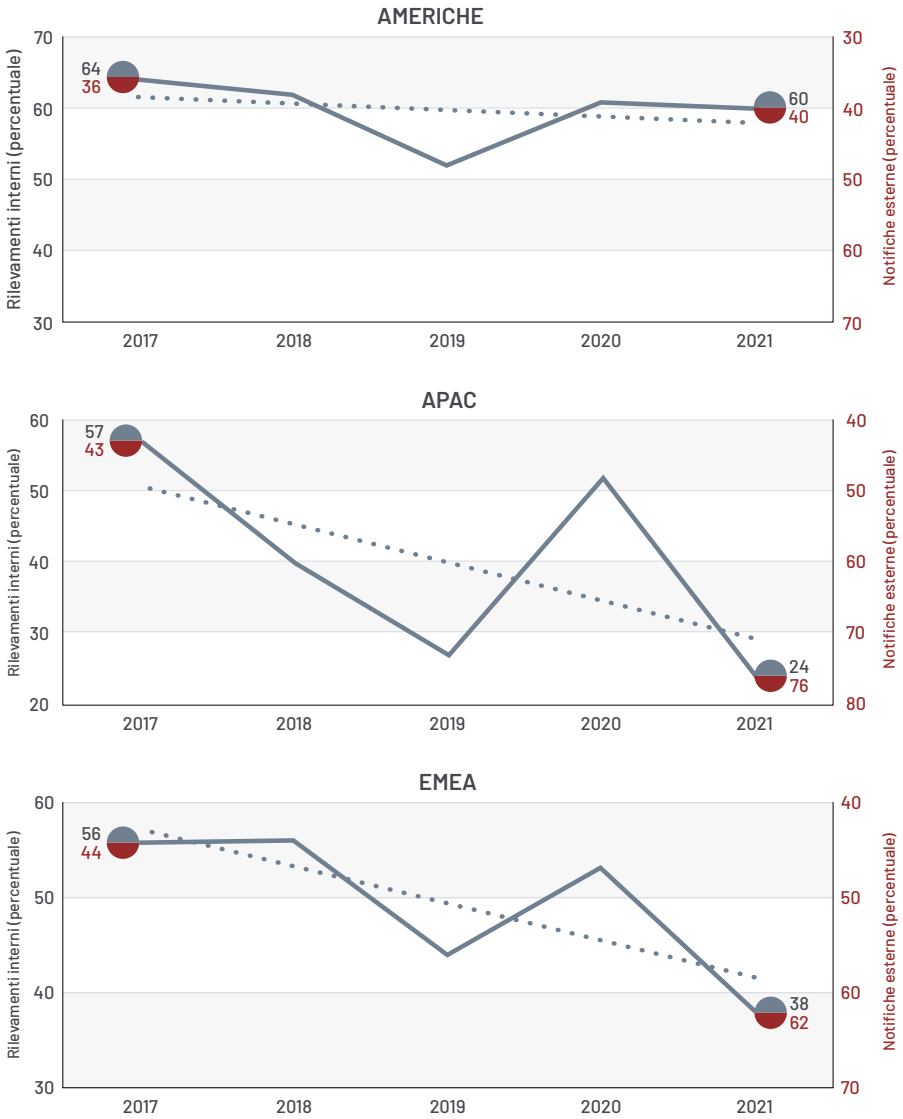


Nelle Americhe le organizzazioni hanno rilevato intrusioni interne nel 60% dei casi nel corso del 2021 rispetto al 61% dei casi nel 2020. Esiste una relativa stabilità nelle tendenze di rilevamento in base alla fonte per le Americhe dal 2017 al 2021.

Le organizzazioni dell'area APAC hanno ricevuto notifica da parte di un'entità esterna nel 76% delle intrusioni nel 2021 rispetto al 48% delle intrusioni nel 2020. Le osservazioni per il 2021 sono in linea con le osservazioni per l'area APAC dal 2019. Nel corso degli ultimi cinque anni, gli esperti Mandiant hanno visto cambiamenti relativamente grandi nel rilevamento delle metriche in base alla fonte per l'area APAC.

Nell'area EMEA le organizzazioni hanno ricevuto notifica di un incidente da un entità esterna nel 62% delle intrusioni del 2021 rispetto al 47% delle intrusioni del 2020. In modo analogo all'area APAC, quando si analizza la tendenza quinquennale, nell'area EMEA rimane la variabilità nel rilevamento in base alla fonte. La variabilità osservata sia per l'area APAC che per l'area EMEA può essere spiegata in parte dalla continua maturazione dei programmi di sicurezza delle organizzazioni, nonché dalla capacità di notifica delle entità esterne in queste regioni.

Rilevamento per fonte per area, 2017–2021



Il **tempo di attesa** viene calcolato in base al numero di giorni in cui un aggressore rimane presente nell'ambiente della vittima prima di essere individuato. La mediana rappresenta un valore al punto medio di un set di dati ordinato per grandezza.

Tempo di attesa

Il tempo di attesa mediano globale ha continuato a migliorare nel 2021, con le organizzazioni che rilevano ora intrusioni in tre settimane. Il tempo di attesa mediano globale per le organizzazioni che hanno appreso del loro incidente di sicurezza attraverso una notifica esterna di terze parti è sensibilmente migliorato nel 2021. Non solo le entità esterne stanno inviando più notifiche di intrusioni alle organizzazioni rispetto al 2020, ma le stanno anche recapitando più rapidamente, con conseguente riduzione dei tempi di attesa. Il tempo di attesa mediano per le intrusioni rilevate internamente si è allungato nel 2021 rispetto al 2020, ma è rimasto più breve del tempo di risposta mediano per le notifiche esterne.

Variazione nel tempo di attesa mediano

24 → **21**

GIORNI NEL 2020 **GIORNI NEL 2021**

Tempo di attesa globale

Il tempo di attesa mediano globale per il 2021 è stato di 21 giorni rispetto ai 24 giorni del 2020. Questo miglioramento del tempo di attesa mediano globale, pari al 13%, comprendeva cambiamenti notevoli in relazione alla fonte di rilevamento. Il tempo di attesa mediano globale per gli incidenti identificati esternamente è diminuito da 73 a 28 giorni. Al contrario, gli incidenti che sono stati identificati internamente hanno visto un allungamento del tempo di attesa mediano globale da 12 a 18 giorni.

Sono stati riscontrati miglioramenti significativi per quanto riguarda il tempo di attesa mediano globale quando la fonte della notifica era un'entità esterna. Le entità esterne stanno ora rilevando intrusioni e informando le organizzazioni in meno di un mese, una velocità del 62% più elevata rispetto al 2020. Questo indica capacità di rilevamento migliorate da parte delle entità esterne, oltre a comunicazioni e programmi di sensibilizzazione più consolidati.

Gli esperti hanno osservato un aumento del 50% del tempo di attesa mediano globale per le intrusioni rilevate internamente. Il tempo di attesa mediano globale per le intrusioni rilevate internamente è aumentato da 12 giorni nel 2020 a 18 giorni nel 2021. Mentre il tempo di attesa mediano per i rilevamenti interni era più lento rispetto al 2020, i rilevamenti interni erano comunque più veloci del 36% rispetto alle notifiche esterne.

Tempo di attesa mediano globale, 2011-2021

Notifiche di compromissione	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Tutte	416	243	229	205	146	99	101	78	56	24	21
Notifica esterna	–	–	–	–	320	107	186	184	141	73	28
Rilevamento interno	–	–	–	–	56	80	57,5	50,5	30	12	18

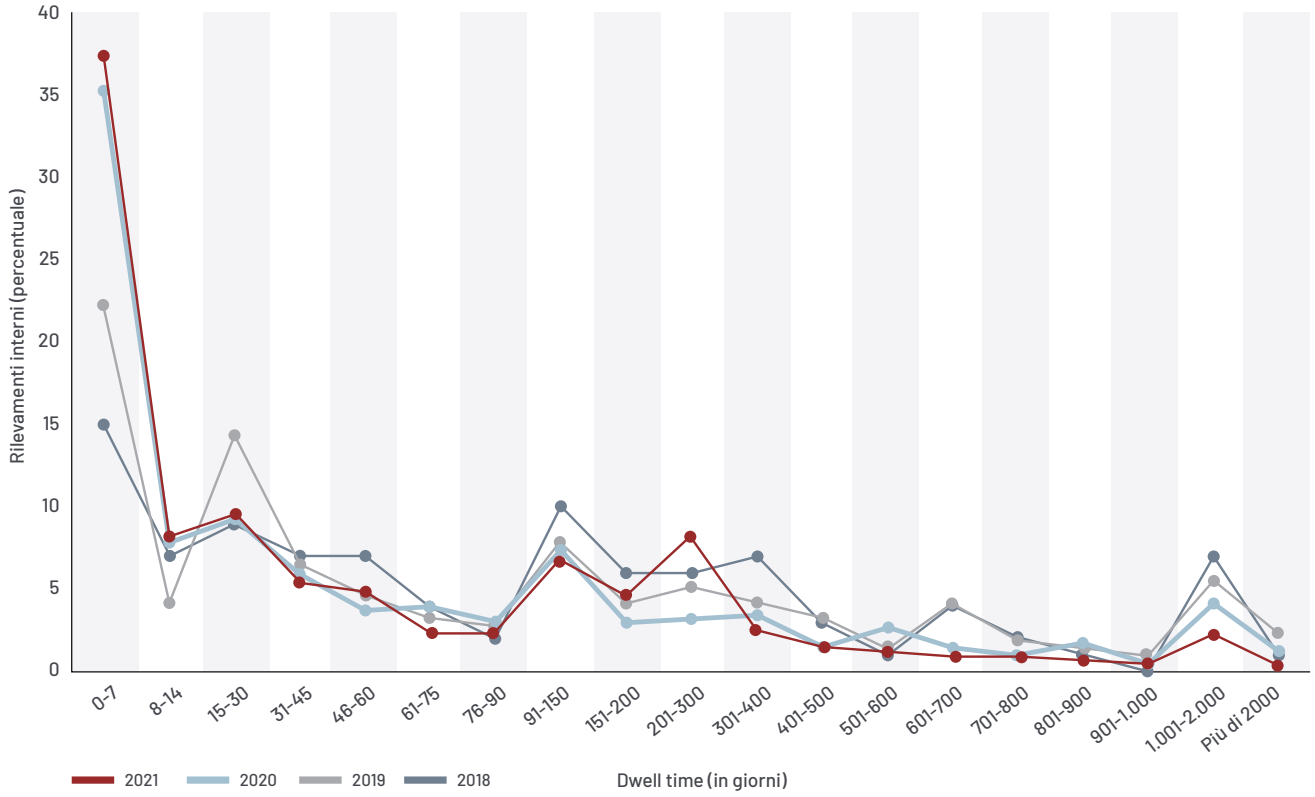
Distribuzione del tempo di attesa globale

La distribuzione del tempo di attesa globale continua a migliorare ad entrambe le estremità dello spettro. Nel 2021, il 55% delle indagini ha registrato un tempo di attesa di 30 giorni o meno, e il 67% di queste (cioè, il 37% delle intrusioni totali) veniva scoperto in una settimana o meno.

Gli esperti Mandiant hanno osservato un picco nei tempi di attesa tra 90 e 300 giorni con il 20% delle indagini incluse in questo intervallo. Ciò potrebbe indicare intrusioni che passano inosservate fino a quando non vengono eseguite azioni di maggiore impatto nell'ambiente dopo le fasi di infezione iniziale e di ricognizione del ciclo di vita dell'attacco mirato. Può anche evidenziare una disparità tra le capacità di rilevamento delle organizzazioni e il tipo di attacchi che queste devono affrontare.

Un minor numero di intrusioni passa inosservato per lunghi periodi di tempo. Solo l'8% delle intrusioni esaminate nel 2021 ha avuto un tempo di attesa di oltre un anno e la metà di queste (il 4% delle intrusioni totali) ha avuto tempo di attesa superiore a 700 giorni.

Distribuzione del tempo di attesa globale, 2018–2021



Variazione nelle indagini riguardanti il ransomware

25% NEL 2020 → **23%** NEL 2021

Nessuna variazione nel tempo di attesa mediano globale: Ransomware

5 GIORNI NEL 2020 → **5** GIORNI NEL 2021

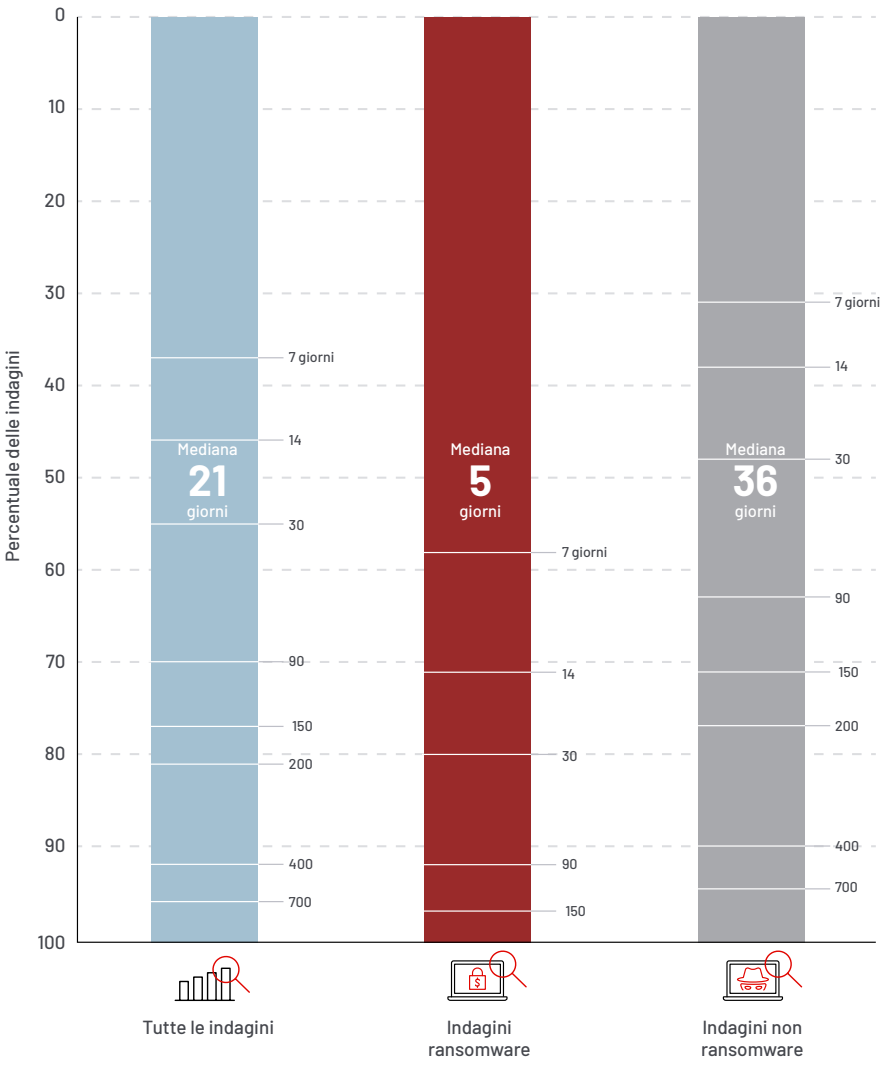
Variazione nel tempo di attesa mediano globale: Non ransomware

45 GIORNI NEL 2020 → **36** GIORNI NEL 2021

Indagini sugli incidenti ransomware

Gli esperti Mandiant hanno osservato che la percentuale di intrusioni che implicano estorsioni di vario tipo e il ransomware è stata relativamente stabile dal 2020 al 2021. Nel 2021 la percentuale di intrusioni che comportava l'uso del ransomware era del 23% rispetto al 25% nel 2020. Questi tipi di attacchi continuano ad essere la forza trainante per la riduzione dei tempi di attesa mediani. Le intrusioni correlate al ransomware avevano un tempo di attesa mediano di 5 giorni rispetto ai 36 giorni delle intrusioni non ransomware, rendendo i tempi di attesa per le intrusioni ransomware un settimo di quelli non ransomware. Mentre il tempo di attesa mediano per le intrusioni correlate al ransomware nel 2021 è rimasto uguale al 2020, gli esperti Mandiant hanno notato una riduzione del 20% del tempo di attesa mediano per le intrusioni non ransomware, anno dopo anno.

Tempo di attesa globale per tipo di indagine, 2021



AMERICHE

Nessuna variazione nel tempo di attesa mediano

17 → **17**

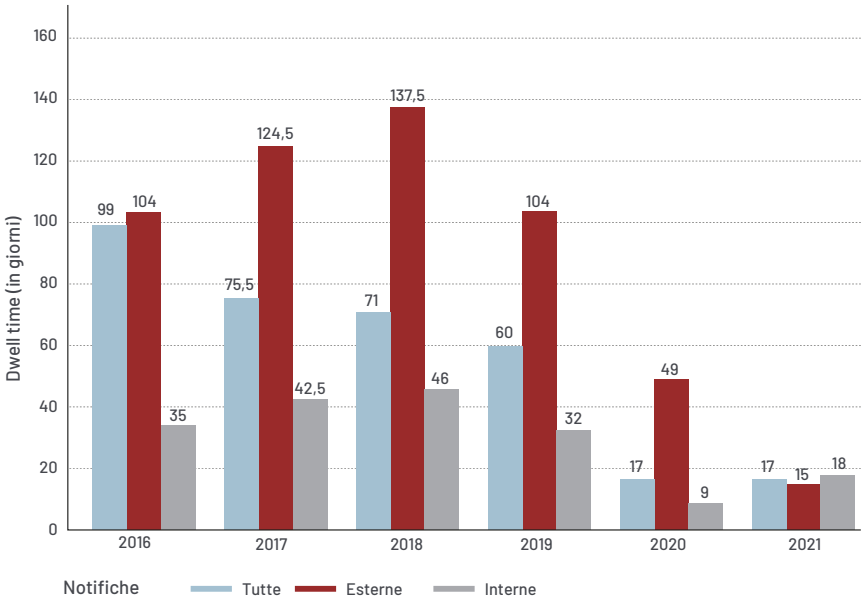
GIORNI NEL 2020 **GIORNI NEL 2021**

Tempo di attesa mediano nelle Americhe

Il tempo di attesa mediano per le intrusioni esaminate nelle Americhe è rimasto costante a 17 giorni nel 2021 rispetto al 2020. Quando è stata considerata la fonte di rilevamento, è stato osservato un aumento di 9 punti percentuali del tempo di attesa mediano per le intrusioni rilevate internamente, passando da 9 giorni del 2020 a 18 giorni del 2021. Mentre il tempo di attesa mediano per il rilevamento interno si è allungato nel 2021 rispetto al 2020, la tendenza a sei anni continua verso rilevamenti interni più veloci. Il tempo di attesa mediano nelle Americhe per i rilevamenti interni nel 2020 ha dimostrato un notevole miglioramento, pertanto non sorprende che questa metrica abbia invertito la tendenza nel 2021.

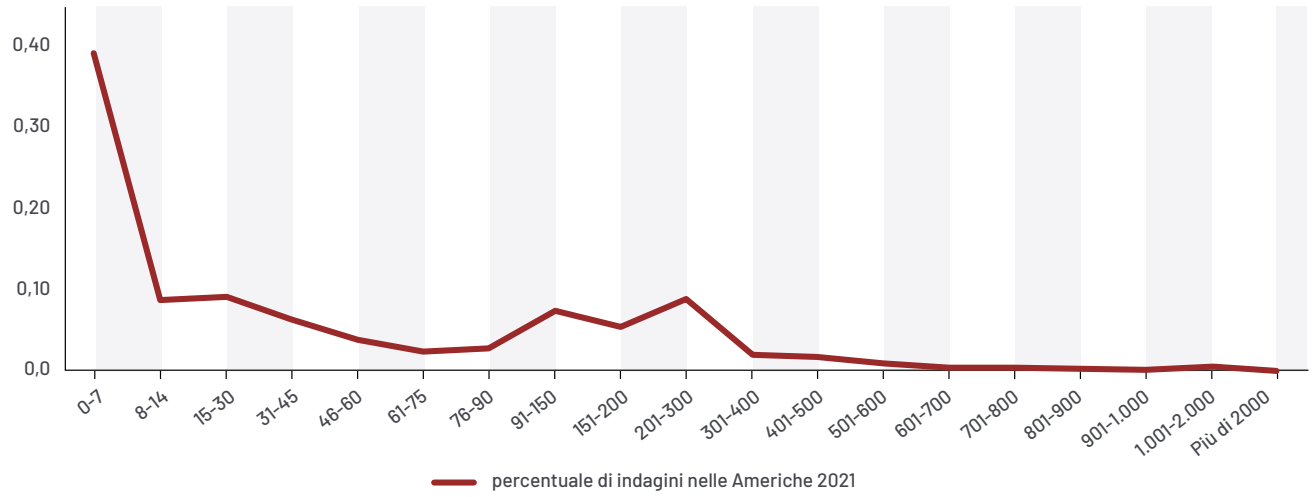
Le intrusioni con una fonte di notifica esterna hanno registrato un tempo di attesa mediano di 49 giorni nel 2020 rispetto a soli 15 giorni nel 2021. Nel 2021 le entità esterne hanno inviato notificate alle organizzazioni nelle Americhe il 69% più velocemente rispetto al 2020.

Tempo di attesa mediano nelle Americhe, 2016-2021



Nelle Americhe il 57% delle intrusioni è stato rilevato in meno di 30 giorni nel 2021 e il 68% di queste intrusioni (il 39% delle intrusioni totali nelle Americhe) è stato rilevato in meno di una settimana. Non solo quasi la metà delle intrusioni viene rilevata in due settimane o meno, ma meno intrusioni stanno passando inosservate per periodi di tempo lunghi. Gli esperti Mandiant hanno osservato un picco nelle intrusioni con i tempi di attesa di 90-300 giorni, rappresentando il 22% delle intrusioni nelle Americhe. Inoltre, solo il 4% delle intrusioni nelle Americhe aveva periodi di attesa superiori a un anno.

Distribuzione del tempo di attesa nelle Americhe, 2021

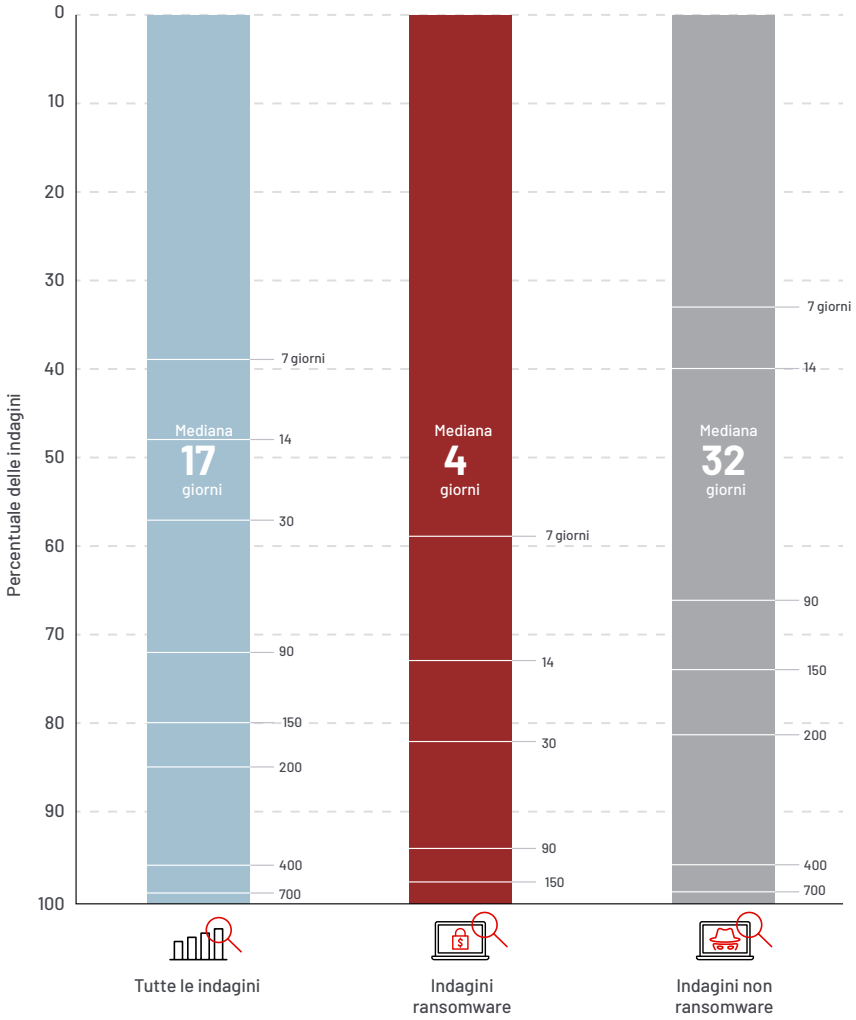


Variazione nelle indagini riguardanti il ransomware

27,5% → **22%**
NEL 2020 NEL 2021

Nel 2021, il 22% delle intrusioni nelle Americhe era correlato al ransomware, una diminuzione di 5,5 punti percentuali rispetto al 2020. Anche se si sono verificate meno intrusioni correlate al ransomware nelle Americhe, queste continuano ad influenzare il tempo di attesa mediano. Le intrusioni ransomware nelle Americhe hanno registrato un tempo di attesa mediano di 4 giorni rispetto ai 32 giorni delle intrusioni non ransomware.

Tempo di attesa per tipo di indagine nelle Americhe, 2021



APAC

Variazione nel tempo di attesa mediano

76 → **21**

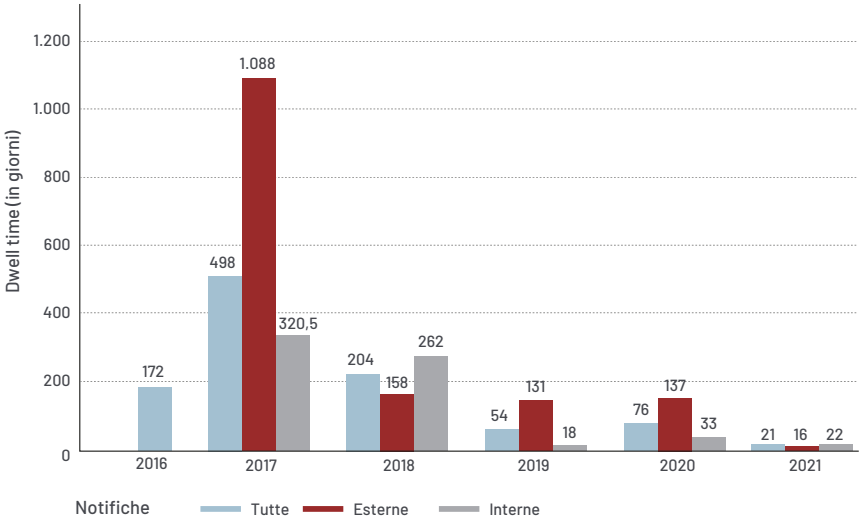
GIORNI NEL 2020 **GIORNI NEL 2021**

Tempo di attesa mediano nell'area APAC

Nel 2021, tutte le metriche del tempo di attesa mediano sono migliorate nell'area APAC. Il tempo di attesa mediano per le intrusioni nell'area APAC è stato di soli 21 giorni nel 2021 rispetto ai 76 giorni del 2020, un miglioramento del 72% di questo tempo, anno dopo anno.

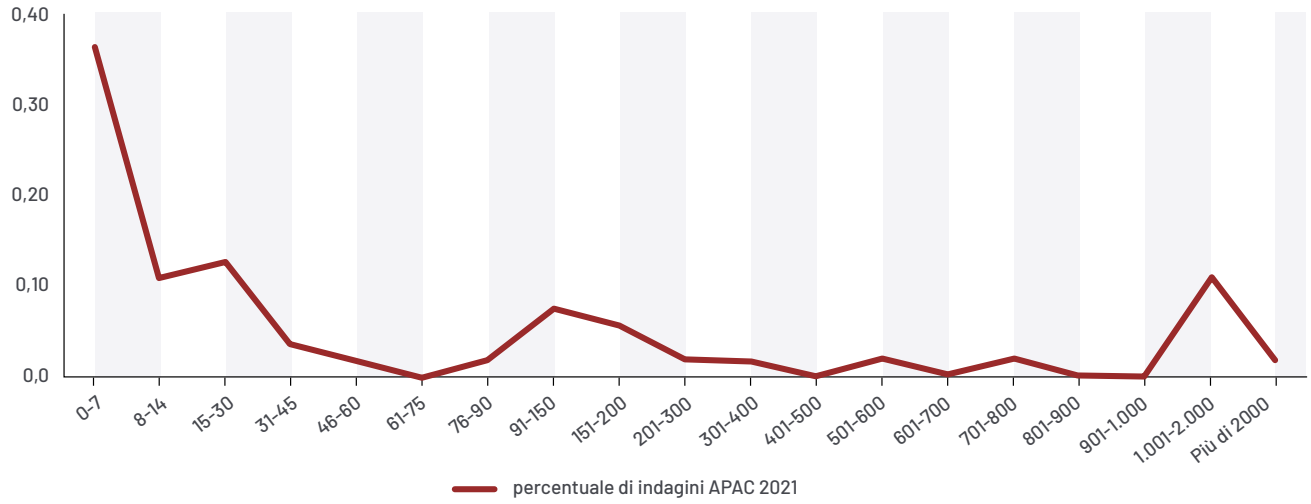
Nell'area APAC le organizzazioni stanno rilevando le intrusioni più rapidamente e le entità esterne stanno avvisando le organizzazioni di intrusioni in minor tempo. Le intrusioni nell'area APAC rilevate internamente hanno registrato un tempo di attesa mediano di 22 giorni nel 2021 rispetto a 33 giorni del 2020. Il tempo di attesa mediano per le intrusioni con una fonte di notifica esterna è stato di 16 giorni nel 2021 rispetto ai 137 giorni del 2020, con una riduzione dell'88%.

Tempo di attesa mediano nell'area APAC, 2016-2021



La distribuzione del tempo di attesa per l'area APAC rivela che il 60% delle intrusioni aveva tempi di attesa di 30 giorni o meno con il 60% di questi (il 36% di tutte le intrusioni nell'area APAC) che veniva rilevato in una settimana o meno. All'altra estremità dello spettro, in modo analogo alle osservazioni degli anni precedenti, la distribuzione del tempo di attesa nell'area APAC continua a mostrare che diverse intrusioni passano inosservate per lunghi periodi di tempo. Gli esperti Mandiant hanno osservato che, nel 2021, il 13% delle intrusioni nell'area APAC aveva tempi di attesa che superavano i tre anni. Le organizzazioni nell'area APAC hanno capacità di rilevamento notevoli. Tuttavia, le intrusioni che inizialmente non vengono rilevate possono passare inosservate, con conseguenti periodi di attesa prolungati prima che vengano finalmente scoperte.

Distribuzione del tempo di attesa nell'area APAC, 2021

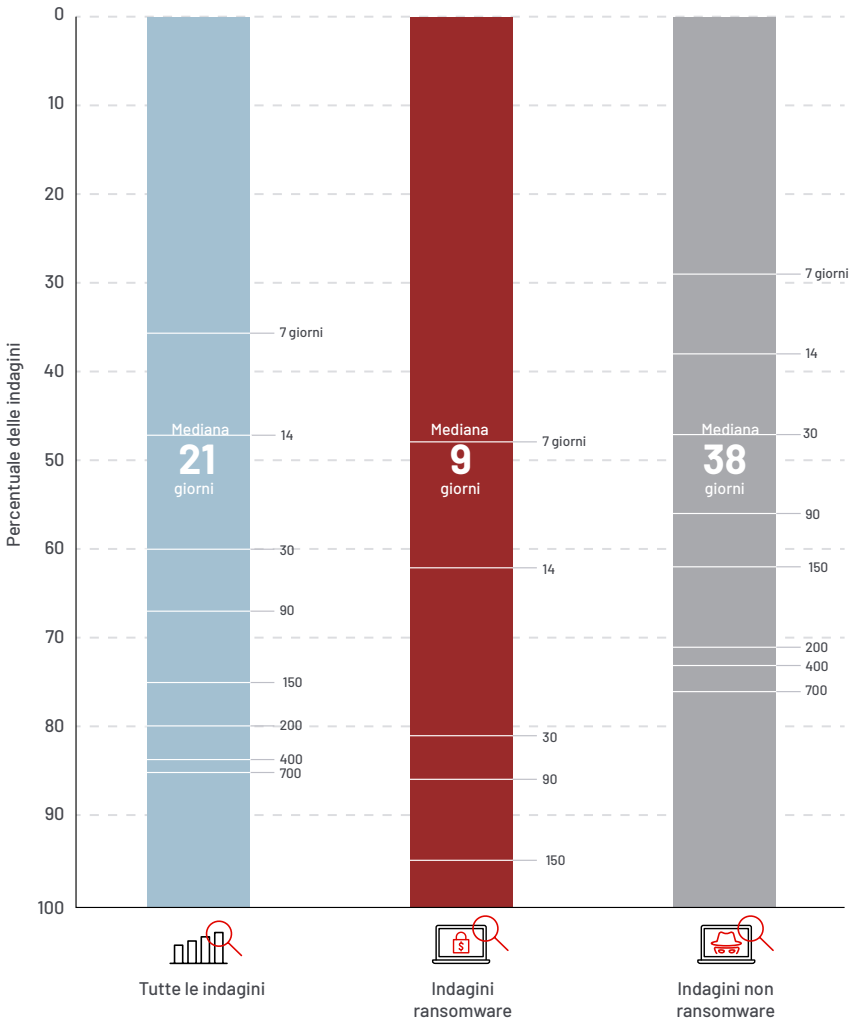


Variazione nelle indagini riguardanti il ransomware

12,5% → **38%**
NEL 2020 NEL 2021

Nell'area APAC gli attacchi ransomware sono stati più diffusi nel 2021 rispetto agli anni precedenti. Le intrusioni correlate al ransomware hanno rappresentato il 38% delle intrusioni esaminate nell'area APAC nel 2021 rispetto al 12,5% di quelle nel 2020 e al 18% di quelle nel 2019. Il tempo di attesa mediano nell'area APAC per le intrusioni correlate al ransomware è stato di 9 giorni rispetto ai 38 giorni delle intrusioni non ransomware.

Tempo di attesa per tipo di indagine, 2021



EMEA

Variazione nel tempo di attesa mediano

66 → **48**

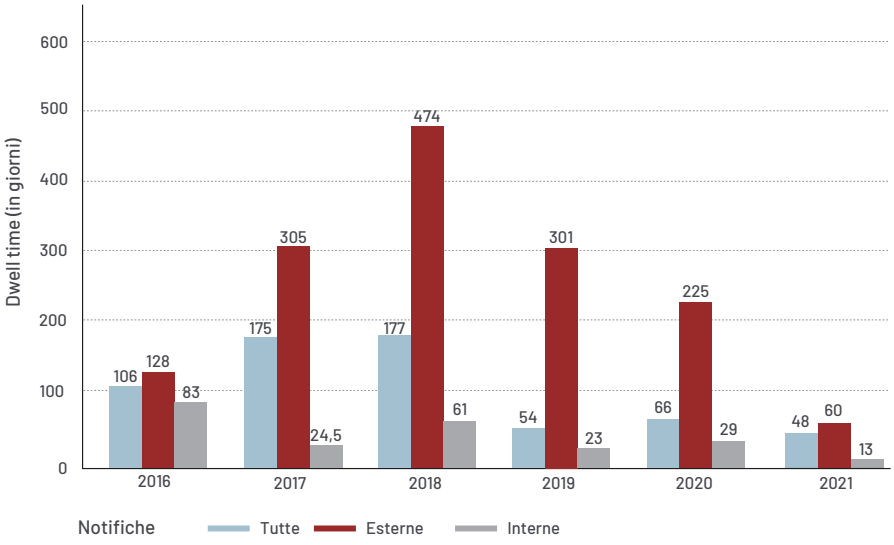
GIORNI NEL 2020 **GIORNI NEL 2021**

Tempo di attesa mediano nell'area EMEA

Nel 2021 l'area EMEA ha mostrato un miglioramento dei tempi di attesa mediani su tutta la linea, con i tempi di attesa più brevi mai osservati per quest'area in tutte le categorie. Il tempo di attesa mediano per le intrusioni esaminate nell'area EMEA è stato di soli 48 giorni nel 2021 rispetto ai 66 giorni nel 2020 e ai 54 giorni nel 2019.

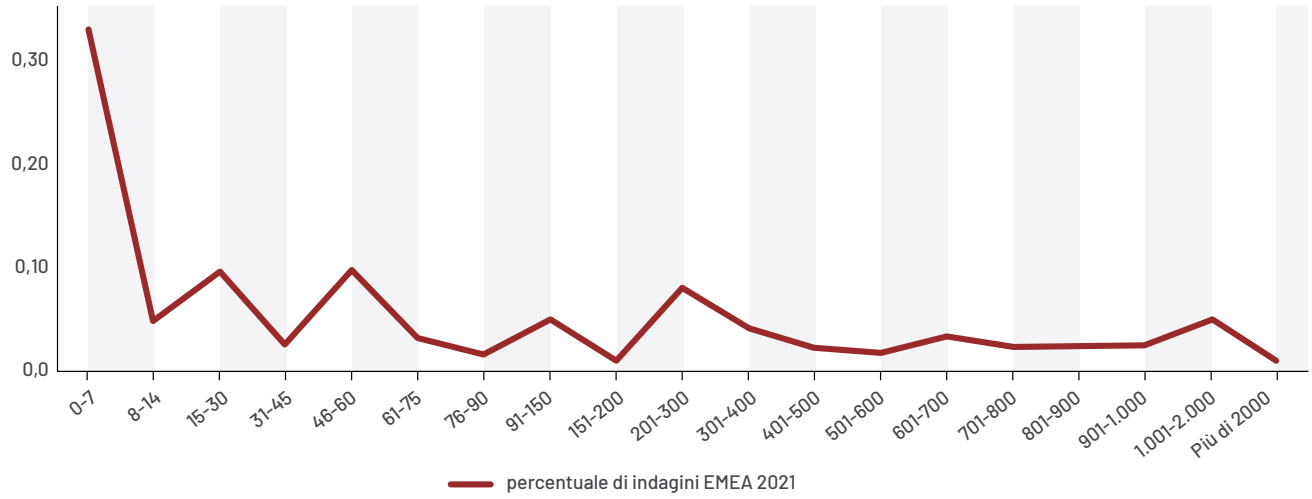
Per le intrusioni rilevate internamente nell'area EMEA, il tempo di attesa mediano è migliorato da 29 giorni nel 2020 a 13 giorni nel 2021. In modo analogo, il tempo di attesa mediano per le intrusioni nell'area EMEA che implicano notifiche esterne è sceso da 225 giorni nel 2020 a 60 giorni nel 2021.

Tempo di attesa mediano nell'area EMEA, 2016-2021



L'esame della distribuzione del tempo di attesa, ha mostrato che il 47% delle intrusioni nell'area EMEA è stato rilevato entro 30 giorni; il 70% di queste intrusioni (il 33% di tutte le intrusioni nell'area EMEA) è stato rilevato entro una settimana. L'area EMEA ha anche mostrato un miglioramento della percentuale di intrusioni con tempi di attesa prolungati. Nel 2021, il 5,5% delle intrusioni nell'area EMEA ha avuto periodi di attesa più lunghi di tre anni, il che rappresenta un miglioramento di 2,5 punti percentuali rispetto al 2020.

Distribuzione del tempo di attesa nell'area EMEA, 2021

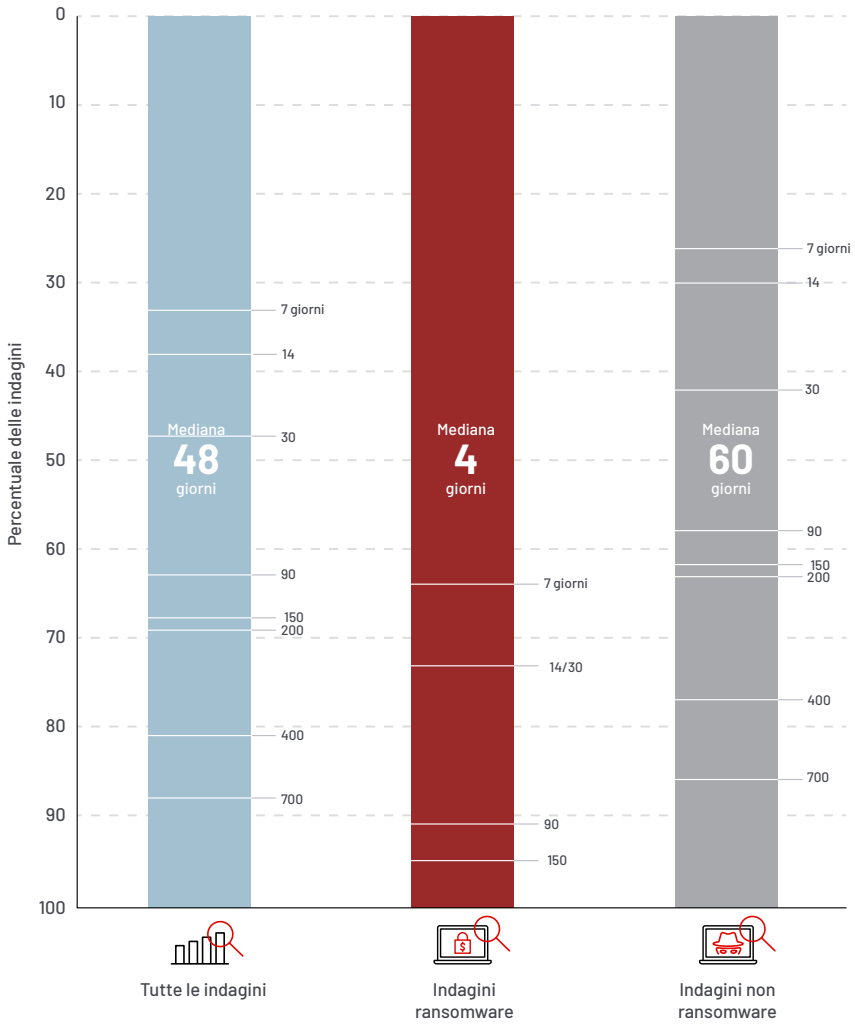


Variazione nelle indagini riguardanti il ransomware

22% → **17%**
NEL 2020 **NEL 2021**

Nel 2021, nell'area EMEA, un minor numero di indagini è stato correlato al ransomware, il 17% rispetto al 22% nel 2020. Tuttavia, la rapidità delle intrusioni ransomware ha contribuito al miglioramento complessivo del tempo di attesa mediano nell'area EMEA. Gli esperti Mandiant hanno osservato che il tempo di attesa mediano del 2021 nell'area EMEA per le intrusioni correlate al ransomware è stato di soli 4 giorni rispetto ai 60 giorni per le intrusioni non ransomware.

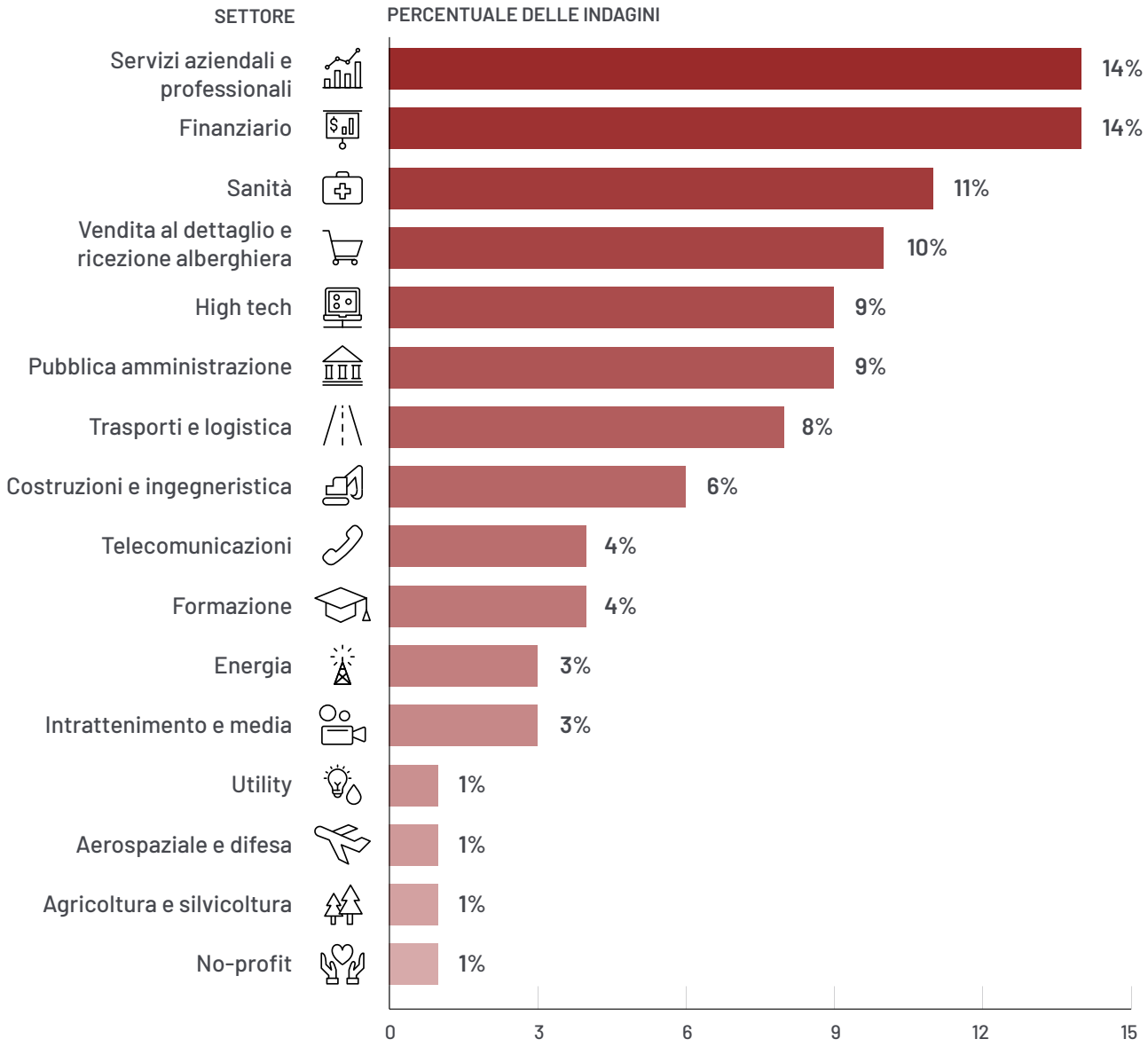
Tempo di attesa per tipo di indagine nell'area EMEA, 2021



Settori presi di mira

Mandiant continua a vedere un accanimento costante contro determinati settori da parte degli aggressori. Nel 2021 i servizi aziendali/professionali e finanziari sono stati i settori più bersagliati del mondo. La vendita al dettaglio e le strutture ricettive, l'assistenza sanitaria e l'alta tecnologia sono i cinque settori preferiti dagli aggressori. Mandiant continua a constatare come questi stessi settori siano presi di mira ogni anno a livello mondiale.

Settori globali presi di mira, 2021



Attacchi mirati

Vettore di infezione iniziale

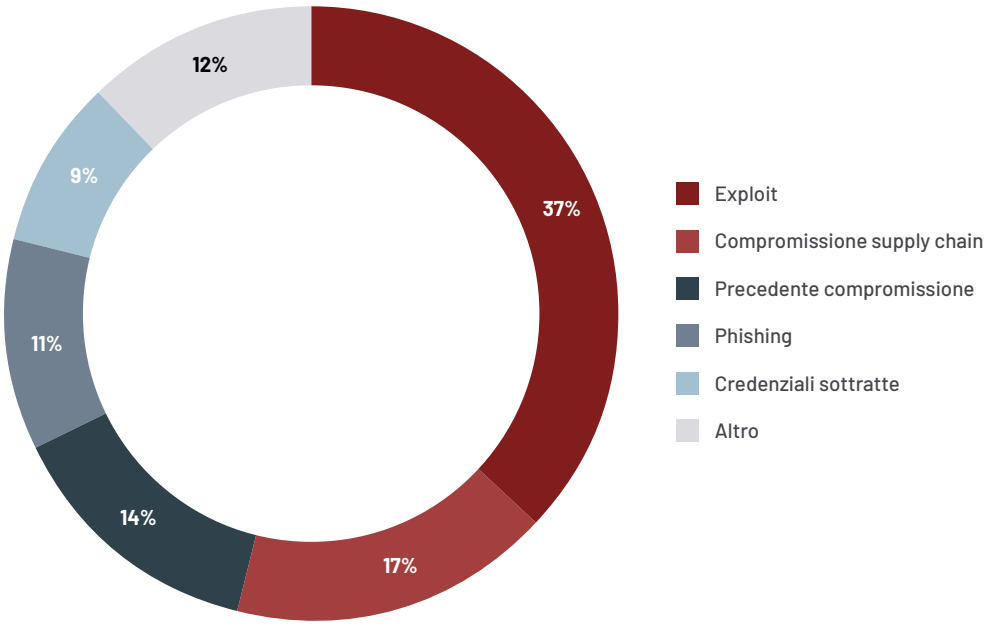
Gli exploit sono rimasti il vettore di infezione iniziale più frequentemente identificato nel 2021. Nelle intrusioni in cui è stato identificato il vettore di infezione iniziale, il 37% è stato avviato con un exploit: un aumento di 8 punti percentuali rispetto al 2020.

La compromissione della supply chain è stata il secondo vettore di infezione iniziale più diffuso identificato nel 2021. Nei casi in cui è stato identificato il vettore di infezione iniziale, la compromissione della supply chain rappresentava il 17% delle intrusioni nel 2021 rispetto a meno dell'1% nel 2020. Inoltre, l'86% delle intrusioni con compromissione della supply chain nel 2021 è stato correlato alla violazione di SolarWinds e a SUNBURST.[1]

Nel 2021 gli esperti Mandiant hanno osservato un aumento delle intrusioni con un vettore di infezione iniziale collegato a una compromissione precedente. Queste intrusioni includono il trasferimento da un gruppo all'altro e infezioni da malware precedenti. Le compromissioni precedenti rappresentavano il 14% delle intrusioni laddove il vettore di infezione iniziale è stato identificato.

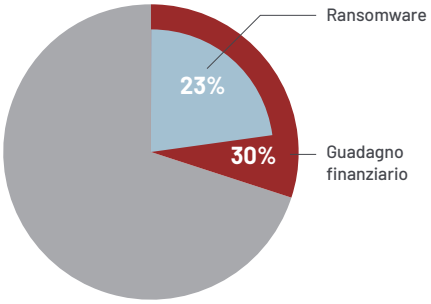
Gli esperti Mandiant hanno osservato molto meno intrusioni iniziate tramite phishing nel 2021. Nei casi in cui è stata identificata la compromissione iniziale, il phishing è risultato essere il vettore solo nell'11% delle intrusioni nel 2021 rispetto al 23% nel 2020. Questo indica la capacità delle organizzazioni di rilevare e bloccare meglio le email di phishing, nonché una migliore formazione sulla sicurezza dei dipendenti per riconoscere e segnalare i tentativi di phishing.

Vettore di infezione iniziale, 2021 *(qualora identificato)*



1. Mandiant (13 dicembre 2021). Aggressore molto sfuggente sfrutta la supply chain SolarWinds per compromettere diverse vittime nel mondo con i backdoor SUNBURST.

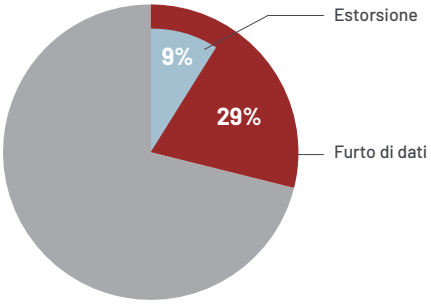
Le attività degli aggressori



Guadagno finanziario

38% NEL 2020 → **30%** NEL 2021

Le intrusioni con motivazione finanziaria continuano ad essere una colonna portante nel 2021, con aggressori che cercano di guadagnare in 3 intrusioni su 10 mediante metodi come estorsione, riscatto, furto di carte di pagamento e bonifici illeciti. La percentuale di intrusioni con motivazione finanziaria è scesa al 30% nel 2021 rispetto al 38% di intrusioni osservate nel 2020. Gli esperti Mandiant hanno osservato una diminuzione di 2 punti percentuali in particolare negli incidenti legati al ransomware nel 2021. Un altro probabile fattore che ha contribuito alla diminuzione delle operazioni finalizzate al guadagno finanziario nel 2021 è stato l'aumento delle azioni legislative di contrasto contro gli attori motivati finanziariamente che ha portato ad arresti, rimozione dei server e appropriazione dei fondi estorti.



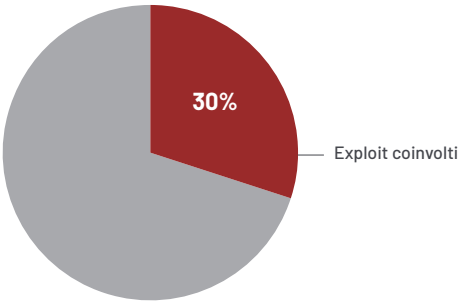
Furto di dati

32% NEL 2020 → **29%** NEL 2021

Gli attori delle minacce continuano a dare priorità al furto di dati come obiettivo primario della loro missione. Nel 2021 Mandiant ha identificato il furto di dati nel 29% delle intrusioni. Nel 32% delle intrusioni che implicano il furto di dati (il 9% di tutte le intrusioni) i dati rubati sono stati specificamente presi di mira per essere utilizzati come arma dell'attore della minaccia durante le negoziazioni per il pagamento. Nel 12% delle intrusioni che implicano il furto di dati (il 4% di tutte le intrusioni) il furto di dati era probabilmente a supporto di obiettivi finali, quali furto di proprietà intellettuale o spionaggio.

Compromissione dell'architettura e minaccia interna

Nel 2021 gli esperti Mandiant hanno osservato un leggero aumento delle compromissioni che sono probabilmente servite solo a compromettere l'assetto dell'architettura per ulteriori attacchi. Nel 2021 questa attività è stata individuata nel 4% delle intrusioni, un aumento di 1 punto percentuale rispetto al 2020. Allo stesso modo, la minaccia interna continua ad essere rara con solo l'1% delle intrusioni analizzate da Mandiant ad essa correlate. Queste metriche sono rimaste relativamente stabili dopo anni di segnalazioni.



Attività di exploit

Gli aggressori hanno spesso sfruttato gli exploit nel 2021, infatti il 30% di tutte le intrusioni hanno comportato attività di exploit. Nel 2021 la maggior parte delle vulnerabilità è stata rilevata in prodotti quali Microsoft Exchange[2 e3], SonicWall Email Security (ES)[4], le appliance Pulse Secure VPN[5] e la utility Apache Log4j 2[6] per citarne alcuni. Gli aggressori hanno sfruttato queste vulnerabilità per iniziare e portare avanti le intrusioni. Gli esperti Mandiant hanno anche osservato gli aggressori sfruttare le vulnerabilità per distribuire ransomware.[7]

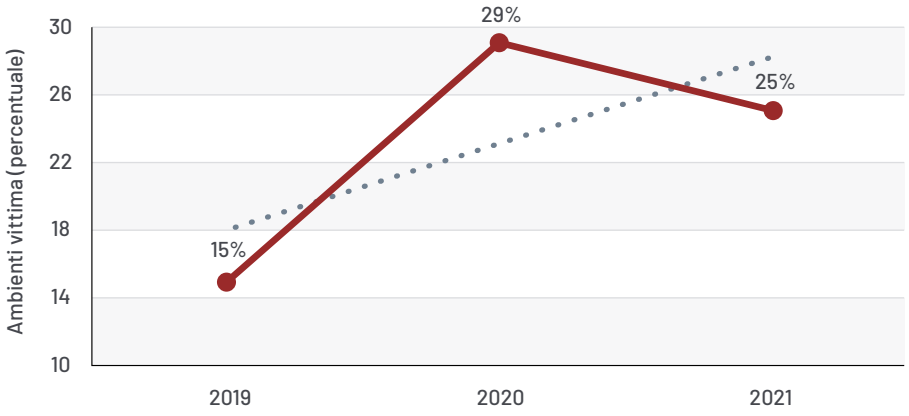
Variazione in più gruppi di aggressori identificati (in base all'ambiente)

29% NEL 2020 → **25%** NEL 2021

Ambiente

Nel 2021 gli esperti Mandiant hanno constatato che un quarto degli ambienti vittima presentava più di un gruppo di minacce distinto. Questi ambienti includevano indagini con gruppi di aggressori che interagivano e ambienti allettanti presi di mira, che attiravano più attori di minacce in modo indipendente. Mentre nel 2021 la percentuale di ambienti vittima con più gruppi di aggressori è diminuita rispetto al 2020, la tendenza triennale mostra una probabile crescita continua.

Più gruppi di aggressori identificati, 2019-2021

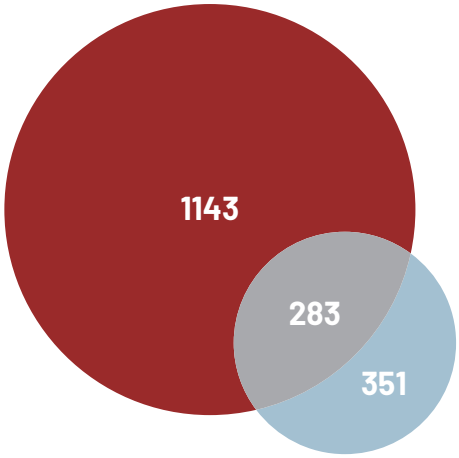


2. Mandiant (4 marzo 2021). Rilevamento e risposta allo sfruttamento delle vulnerabilità del giorno zero di Microsoft Exchange.
3. Mandiant (17 novembre 2021). ProxyNoShell: un cambiamento nelle tattiche di sfruttamento delle vulnerabilità di ProxyShell.
4. Mandiant (20 aprile 2021). Sfruttamento del giorno zero di SonicWall Email Security porta alla compromissione di aziende.
5. Mandiant (20 aprile 2021). Controlla la tua rete Pulse: Gli aggressori APT sospettati sfruttano tecniche di bypass per l'autenticazione e il giorno zero di Pulse Secure
6. Mandiant (15 dicembre 2021). Sfruttamento iniziale di Log4Shell e consigli di mitigazione.
7. Mandiant (23 febbraio 2021). (S)cambio di pace: osservando il gruppo UNC2596 nello Sfruttamento delle vulnerabilità per distribuire i ransomware a Cuba.

Gruppi di aggressori

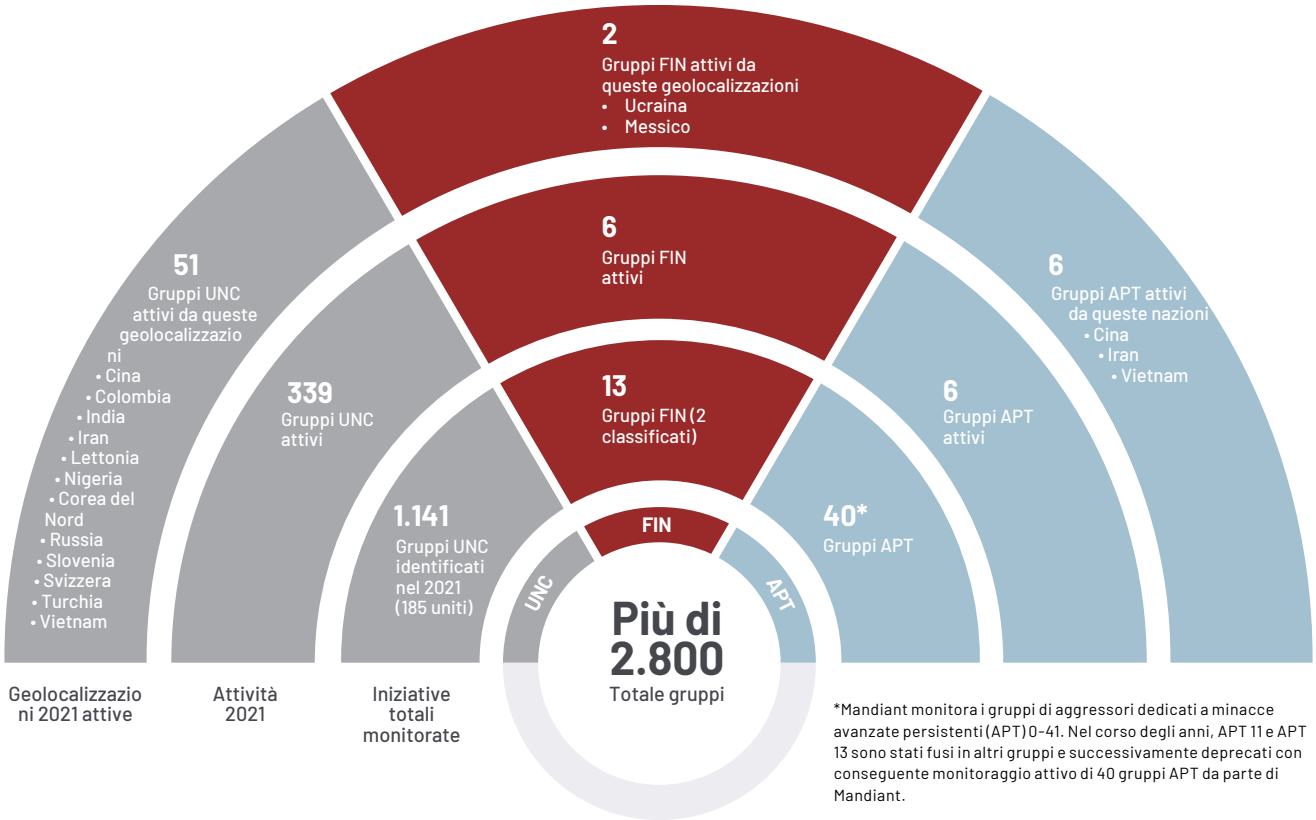
Gli esperti Mandiant tengono attualmente traccia di oltre 2.800 gruppi di aggressori, che includono più di 1.100 gruppi di aggressori appena monitorati per questo periodo di riferimento nel report ***M-Trends***. Mandiant continua ad espandere la sua vasta base di conoscenze sugli attori delle minacce attraverso il raggruppamento e l'attribuzione delle attività degli aggressori osservati non solo durante le indagini in prima linea, ma anche dall'analisi di report pubblici, dalla condivisione di informazioni e da altre ricerche.

Nel 2021 gli esperti Mandiant hanno classificato due gruppi di aggressori denominati FIN12[8] e FIN13.[9] Inoltre, ha unito 185 gruppi di aggressori in altri gruppi, basandosi su un'ampia ricerca nelle sovrapposizioni delle attività. Per i dettagli sulle modalità di definizione, riferimento e fusione dei gruppi UNC da parte di Mandiant, vedere la sezione "Modalità con cui Mandiant monitora gli attori di minacce non classificati".[10]



- Monitoraggio di nuovi gruppi di aggressori nel 2021
- Monitoraggio e osservazione di nuovi gruppi di aggressori nel 2021
- Gruppi di aggressori osservati nel 2021

Gruppi di aggressori 2021



*Mandiant monitora i gruppi di aggressori dedicati a minacce avanzate persistenti (APT) 0-41. Nel corso degli anni, APT 11 e APT 13 sono stati fusi in altri gruppi e successivamente deprecati con conseguente monitoraggio attivo di 40 gruppi APT da parte di Mandiant.

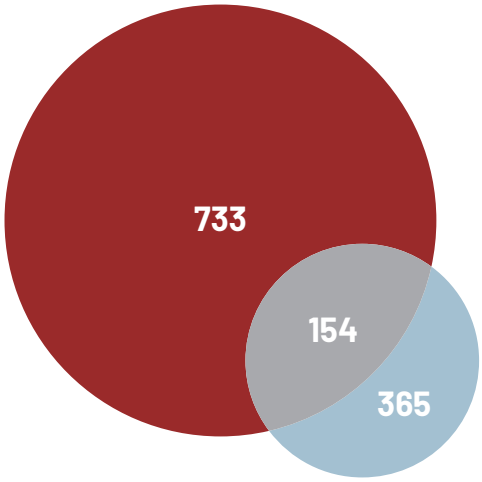
8. Mandiant (7 ottobre 2021). FIN12: il prolifico aggressore mediante intrusioni ransomware che ha preso di mira in maniera aggressiva obiettivi nel settore sanitario
9. Mandiant (7 dicembre 2021). FIN13: un aggressore cybercriminale focalizzato sul Messico
10. Mandiant (17 dicembre 2020). DebUNCing Attribution: modalità con cui Mandiant monitora gli aggressori non classificati

Malware

Mandiant espande continuamente il suo patrimonio di conoscenze sul malware basandosi sulle intuizioni acquisite dalle prime linee degli incidenti informatici, dai report pubblici e da vari altri percorsi di ricerca. Nel 2021 Mandiant ha iniziato a monitorare oltre 700 nuove famiglie di malware. Questo numero continua a crescere in linea con le tendenze precedenti senza alcun segno di rallentamento.

Nel 2021 gli esperti Mandiant hanno osservato gli aggressori utilizzare 365 famiglie di malware differenti durante l'esame degli ambienti compromessi. Questo numero continua a crescere in linea con il numero di famiglie di malware osservate rispetto agli anni precedenti. Delle quasi 365 famiglie di malware osservate dagli esperti Mandiant durante le intrusioni, 154 erano famiglie di malware che Mandiant aveva iniziato a monitorare nel 2021.

Una famiglia di malware è un programma o una serie di programmi, con un sufficiente "code overlap" e che Mandiant considera quindi appartenenti alla stessa "famiglia". Il termine famiglia amplia l'ambito d'azione di un singolo elemento di malware in quanto può essere modificato nel corso del tempo, andando a creare così nuove versioni.



- Nuove famiglie di malware monitorate nel 2021
- Nuove famiglie di malware monitorate e osservate nel 2021
- Famiglie di malware osservate nel 2021

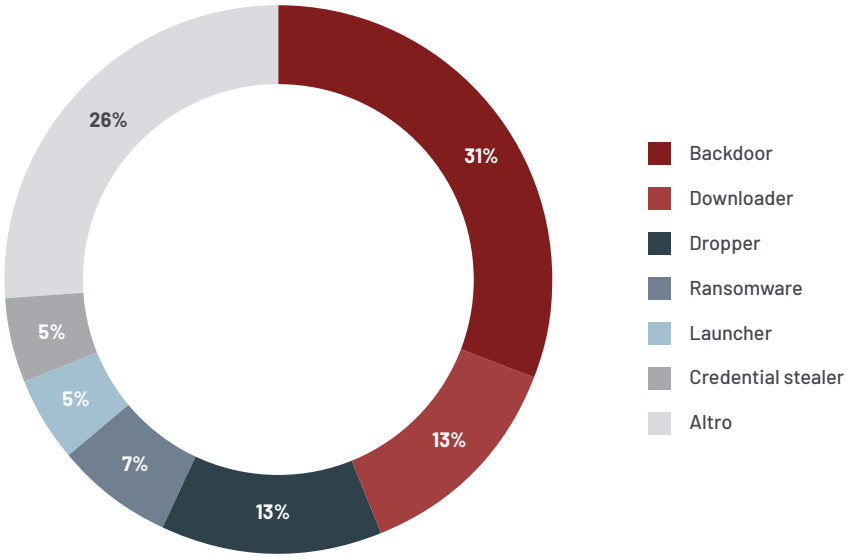
Famiglie di malware per categoria

Delle 733 nuove famiglie di malware monitorate nel 2021, tra le prime cinque categorie c'erano le backdoor (31%), i downloader (13%), i dropper (13%), i ransomware (7%), i launcher (5%) e i programmi di intercettazione delle credenziali (5%). Queste categorie rimangono coerenti con gli anni precedenti.

Una categoria di malware descrive lo scopo principale della famiglia di malware. A ogni famiglia di malware viene assegnata una sola categoria che ne descrive meglio lo scopo principale, indipendentemente dal fatto che essa possa rientrare in più categorie.

Categoria di malware	Scopo principale
Backdoor	Un programma il cui scopo principale è consentire all'attaccante di inviare comandi in modo interattivo al sistema su cui è installato.
Credential stealer	Una utility il cui scopo principale è accedere, copiare o rubare le credenziali di autenticazione.
Downloader	Un programma il cui unico scopo è scaricare (e forse lanciare) un file da un indirizzo specificato, ma che non fornisce alcuna funzionalità aggiuntiva, né supporta altri comandi interattivi.
Dropper	Un programma il cui scopo principale è estrarre, installare e potenzialmente lanciare o eseguire uno o più file.
Launcher	Un programma il cui scopo principale è lanciare uno o più file. Si differenzia da un dropper o da un installer in quanto non contiene o non configura il file, ma si limita a eseguirlo o caricarlo.
Ransomware	Un programma il cui scopo principale è eseguire alcune azioni dannose (es. crittografia dei dati), con l'obiettivo di estorcere un pagamento alla vittima affinché possa evitare o annullare l'azione dannosa.
Altro	Include tutte le altre categorie di malware, come utility, keylogger, punto vendita (POS), tunneler e data miner.

Nuove famiglie di malware monitorate per categoria, 2021



Una famiglia di malware osservata è una famiglia di malware identificata durante un'indagine condotta dagli esperti Mandiant.

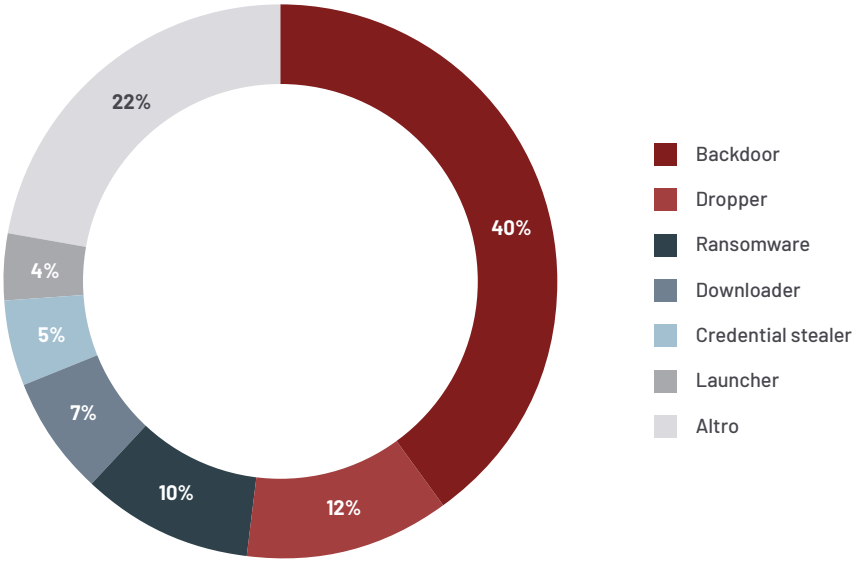
Famiglie di malware osservate per categoria

Le backdoor continuano ad essere gli attacchi preferiti dagli aggressori e includono costantemente la più grande categoria di famiglie di malware osservata durante le indagini Mandiant nel corso degli anni. Delle 365 famiglie di malware osservate nel 2021, le categorie principali includevano backdoor (40%), dropper (12%), ransomware (10%), downloader (7%), programmi di intercettazione delle credenziali (5%) e launcher (4%).

In modo analogo alle nuove famiglie di malware monitorate, il 22% delle famiglie di malware osservate nel 2021 è stato incluso nella categoria di famiglie di malware "Altro". Rispetto agli anni precedenti, questo numero rimane stabile in quanto gli aggressori creano e utilizzano una varietà di strumenti diversi per portare avanti le loro missioni.

Mandiant ha osservato un aumento nella varietà di famiglie di malware ransomware utilizzate dagli aggressori, che ha accresciuto la popolazione osservata dall'8% nel 2020 al 10% nel 2021.

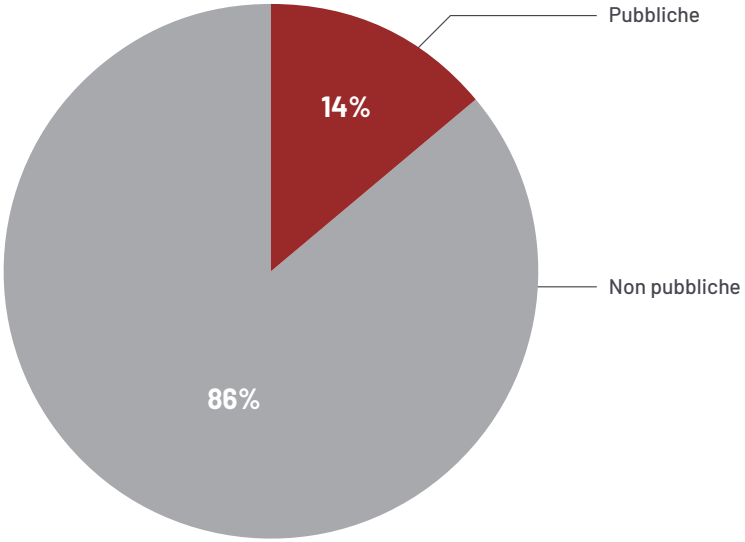
Famiglie di malware osservate per categoria, 2021



Una famiglia di strumenti o codici pubblicamente disponibile può essere ottenuta immediatamente senza restrizioni. Questo comprende strumenti liberamente accessibili su Internet, nonché strumenti che vengono venduti o acquistati, a condizione che possano essere comperati da qualsiasi acquirente.

Nuove famiglie di malware monitorate per disponibilità, 2021

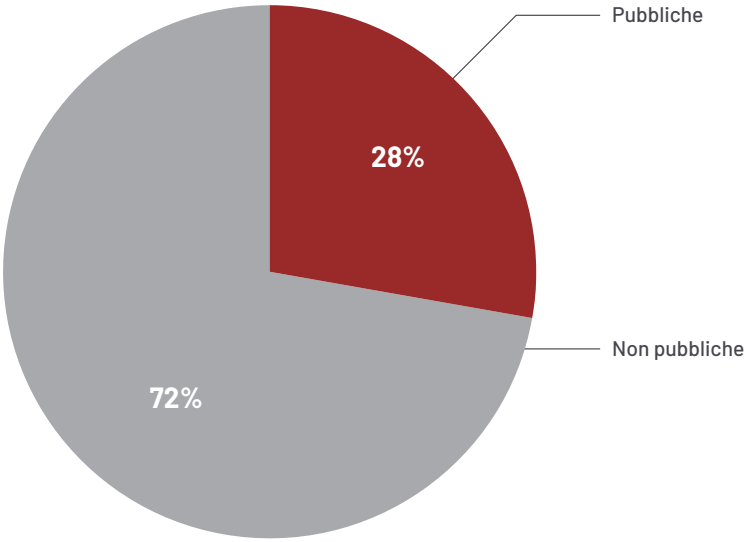
Gli esperti Mandiant hanno osservato che l'86% delle nuove famiglie di malware monitorate non era pubblico, mentre il 14% era pubblicamente disponibile. La maggior parte delle nuove famiglie di malware monitorate continua la tendenza di disponibilità limitata o la probabilità di sviluppo privato.



Una famiglia di strumenti o codici non pubblica non è, in base alle nostre conoscenze, disponibile in forma pubblica (né gratuitamente, né a pagamento). Può includere strumenti sviluppati, posseduti o utilizzati privatamente, nonché strumenti che vengono condivisi o venduti a un limitato numero di clienti.

Famiglie di malware osservate per disponibilità, 2021

In modo analogo alla disponibilità delle nuove famiglie di malware monitorate, nel 2021 gli esperti Mandiant hanno riscontrato che il 72% delle famiglie di malware utilizzate dagli aggressori durante le intrusioni non era pubblico, mentre il 28% era pubblicamente disponibile. Per compiere le loro missioni mediante le intrusioni, gli aggressori utilizzano i malware disponibili sia pubblicamente che non pubblicamente. Mentre molti aggressori utilizzano spesso le stesse famiglie di malware disponibili pubblicamente come BEACON, Mandiant continua a vedere gli aggressori innovarsi e adattarsi per essere efficaci negli ambienti vittima.



Variazione nell'utilizzo di BEACON

24% → **28%**

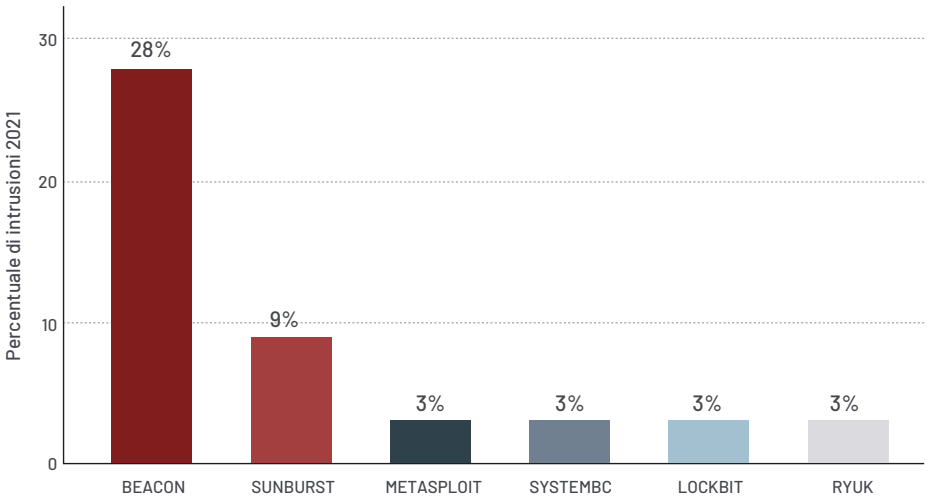
DI INTRUSIONI NEL 2020 **DI INTRUSIONI NEL 2021**

Famiglie di malware osservate con maggiore frequenza

Le famiglie di malware osservate con maggiore frequenza durante le intrusioni esaminate dagli esperti Mandiant includono BEACON, SUNBURST, METASPLOIT, SYSTEMBC, LOCKBIT e RYUK. BEACON è stata ancora una volta la famiglia di malware maggiormente osservata nel 2021, con un'incidenza tre volte superiore rispetto alla seconda famiglia di malware rilevata con maggior frequenza. Inoltre, l'uso di BEACON nelle intrusioni è aumentato dal 24% nel 2020 al 28% nel 2021. BEACON rimane di gran lunga la famiglia di malware preferita tra gli aggressori e Mandiant si aspetta un probabile aumento del suo utilizzo negli anni a venire.

SUNBURST[12] è stato osservato nel 9% di tutte le intrusioni esaminate da Mandiant nel 2021. SUNBURST è stato distribuito su larga scala negli ambienti vittima di tutto il mondo attraverso un aggiornamento dannoso, che ha determinato una compromissione diffusa dell'accesso. Questa metrica è in linea con la relazione osservata tra il secondo vettore di infezione iniziale più diffuso, le compromissioni della supply chain e l'uso di SUNBURST nelle intrusioni.

Famiglie di malware identificate con maggiore frequenza, 2021



RYUK e LOCKBIT sono state le famiglie di ransomware più utilizzate durante le intrusioni esaminate da Mandiant nel 2021. In particolare, la recentemente classificata FIN12[13] ha sfruttato RYUK, BEACON, SYSTEMBC e METASPLOIT per effettuare alcune delle intrusioni più prolifiche osservate in tutto il 2021. Le famiglie di ransomware continuano a contribuire alla raccolta di famiglie di malware ogni anno.

Gli aggressori continuano a utilizzare una varietà di malware per portare avanti le loro missioni. Nel 2021 Mandiant ha osservato che solo il 3,8% delle famiglie di malware veniva utilizzato in 10 o più intrusioni, mentre l'81% delle famiglie di malware è stato osservato solo in una o due intrusioni. Nel corso degli anni, Mandiant ha rilevato che gli strumenti degli aggressori diventano più differenziati mentre questi continuano ad evolversi. Tale diversificazione è dimostrata dalla continuazione di una limitata riorganizzazione tra le intrusioni.

12. Mandiant (13 dicembre 2020). FIN12: aggressore molto sfuggente sfrutta la supply chain SolarWinds per compromettere diverse vittime nel mondo con i backdoor SUNBURST
13. Mandiant (7 ottobre 2021). FIN12: il prolifico aggressore mediante intrusioni ransomware che ha preso di mira in maniera aggressiva obiettivi nel settore sanitario

Definizioni di malware

BEACON è una backdoor disponibile in commercio come parte della piattaforma software Cobalt Strike, comunemente utilizzata per eseguire i test di penetrazione negli ambienti di rete. Il malware è dotato di diverse funzionalità, come ad esempio iniettare ed eseguire un codice arbitrario, caricare e scaricare file ed eseguire i comandi di shell. Mandiant ha visto BEACON utilizzato in una vasta gamma di gruppi di aggressori identificati, tra cui APT19, APT32, APT40, APT41, FIN6, FIN7, FIN9, FIN11, FIN12 e FIN13, oltre a quasi 650 gruppi UNC.

SUNBURST è una backdoor basata su .NET che inizialmente comunica tramite DNS. SUNBURST genera il dominio del server remoto iniziale utilizzando un algoritmo di generazione dei domini. La risposta del DNS restituisce un record CNAME contenente il dominio del server C2 utilizzato per la successiva comunicazione tramite HTTP. I comandi backdoor supportati includono il download, l'esecuzione e la gestione dei file, la manipolazione del registro e la terminazione dei processi. SUNBURST può inoltre disabilitare servizi mirati per evitare il rilevamento e caricare informazioni di base sul sistema che includono l'indirizzo IP di sistema, la configurazione DHCP e le informazioni sul dominio. Mandiant ha osservato lo sfruttamento in corso di SUNBURST da parte di UNC2452.[14]

METASPLOIT è una piattaforma per test di penetrazione che consente agli utenti di identificare, sfruttare e convalidare le vulnerabilità. Mandiant ha riscontrato l'utilizzo di METASPLOIT da parte di APT40, APT41, FIN6, FIN7, FIN11, FIN12, FIN13 e 40 gruppi UNC con obiettivi finali che vanno dallo spionaggio, al guadagno finanziario, fino ai test di penetrazione.

SYSTEMBC è un tunneler scritto in linguaggio C che recupera i comandi correlati al proxy da un server C2 utilizzando un protocollo binario personalizzato su TCP. Un server C2 istruisce SYSTEMBC di agire come proxy tra il server C2 e un sistema remoto. SYSTEMBC è anche in grado di recuperare ulteriori payload via HTTP. A questo scopo, alcune varianti possono utilizzare la rete Tor. I payload scaricati possono essere scritti su disco o mappati direttamente alla memoria prima dell'esecuzione. SYSTEMBC viene spesso utilizzato per nascondere il traffico di rete associato ad altre famiglie di malware. Le famiglie osservate includono DANABOT, SMOKELOADER e URSNIF. Mandiant ha riscontrato l'utilizzo di SYSTEMBC da parte di FIN12 e di ben 10 gruppi UNC con obiettivi legati al guadagno finanziario.

LOCKBIT è un ransomware scritto in linguaggio C che cripta i file memorizzati in locale e sulle condivisioni di rete. LOCKBIT è anche in grado di identificare altri sistemi su una rete e propagarsi tramite SMB. Prima di crittografare i file, LOCKBIT cancella i registri degli eventi, elimina le copie occulte dei volumi e termina i processi e i servizi che possono influire sulla sua capacità di eseguire la crittografia. LOCKBIT è stato osservato utilizzare l'estensione ".lockbit" per i file crittografati. Mandiant ha visto LOCKBIT utilizzato da oltre 10 gruppi UNC con obiettivi di guadagno finanziario e spionaggio.

RYUK è un ransomware scritto in linguaggio C che cripta i file memorizzati sulle unità locali e sulle condivisioni di rete. Rileva anche i file di backup e le copie occulte del volume. Alcune varianti di RYUK possono propagarsi ad altri sistemi di una rete. Mandiant ha visto RYUK utilizzato dai gruppi FIN6 e FIN12 e da 10 gruppi UNC motivati finanziariamente.

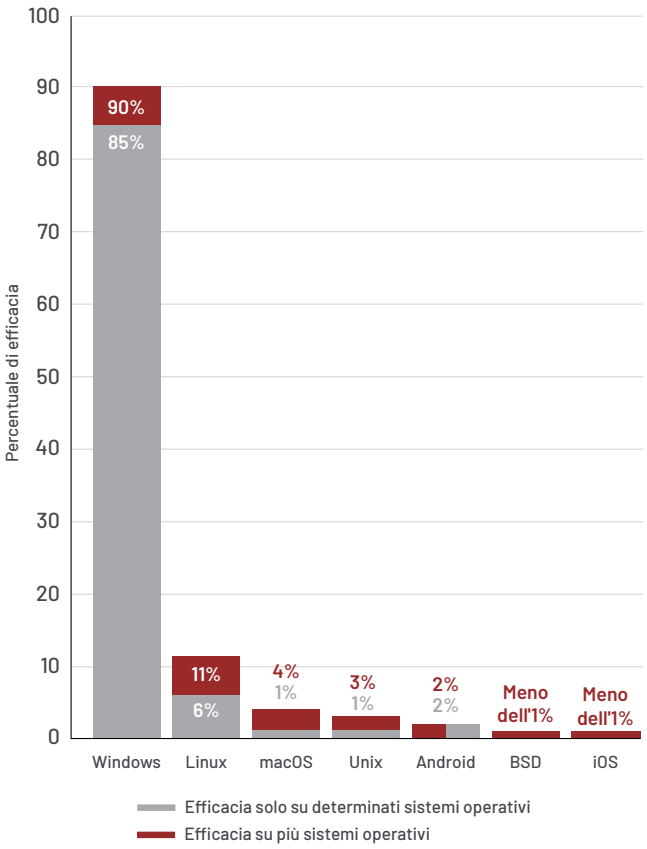
14. Per ulteriori informazioni, visitare il Centro risorse sulle violazioni di SolarWinds

L'efficacia sui sistemi operativi di una famiglia di malware è rappresentata dai sistemi operativi contro cui il malware può essere utilizzato.

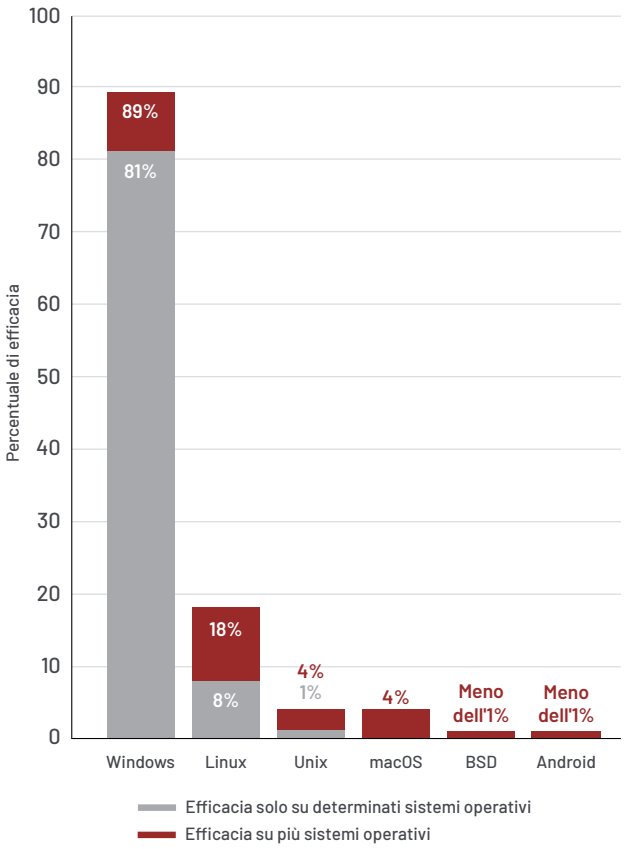
Efficacia sui sistemi operativi

Le tendenze precedenti relative all'efficacia sui sistemi operativi sono proseguite nel 2021, in quanto le nuove famiglie di malware monitorate e osservate sono state prevalentemente efficaci su Windows. Tuttavia, le famiglie di malware che colpiscono Linux sono diventate più diffuse nel 2021. Le nuove famiglie di malware monitorate, che risultano efficaci su Linux, sono aumentate all'11% nel 2021 rispetto all'8% del 2020. Inoltre, le famiglie di malware osservate, efficaci su Linux, sono aumentate al 18% nel 2021 dal 13% nel 2020. L'aumento dell'efficacia su Linux sia delle nuove famiglie di malware monitorate che di quelle osservate dimostra la capacità e la volontà degli aggressori di sviluppare e colpire ambienti con sistemi operativi differenti. Nelle intrusioni analizzate da Mandiant gli aggressori continuano a prendere di mira i sistemi operativi con la stessa attenzione relativa.

Efficacia delle nuove famiglie di malware monitorate per sistema operativo, 2021



Efficacia delle famiglie di malware osservate per sistema operativo, 2021



Tecniche di attacco

Mandiant continua a sostenere gli sforzi della comunità e del settore mappando le proprie scoperte nel framework MITRE ATT&CK. Nel 2021, MITRE ha rilasciato le versioni 9 e 10 di ATT&CK, che si sono concentrate sull'avanzamento della copertura di MITRE per Linux, macOS e delle tecniche dei container. Nel 2021 Mandiant ha mappato oltre 300 tecniche aggiuntive Mandiant nel framework MITRE ATT&CK, portando il totale a più di 2.100 tecniche Mandiant e risultati successivi associati a MITRE ATT&CK.

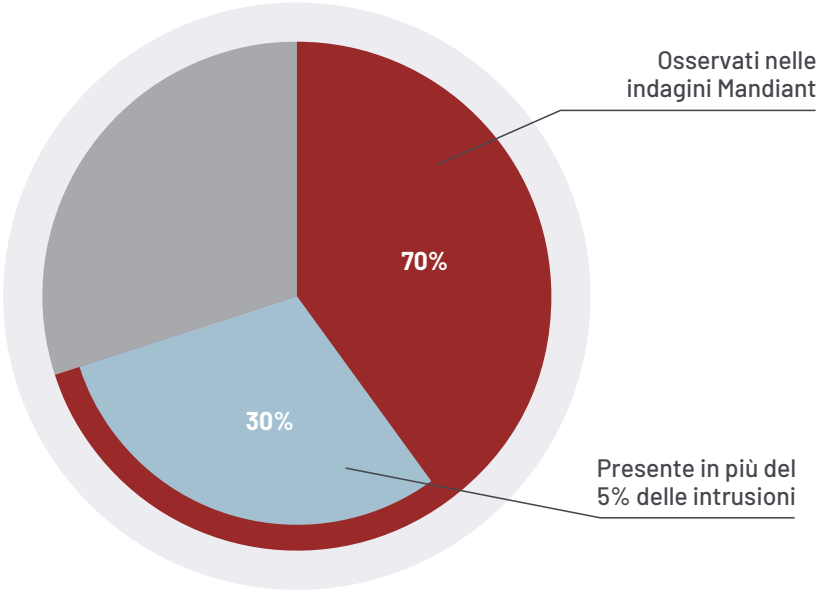
Le organizzazioni devono stabilire le priorità delle misure di sicurezza da implementare e la probabilità che vengano utilizzate tecniche specifiche durante un'intrusione dovrebbe influire su questo processo decisionale. Esaminando la prevalenza dell'uso delle tecniche durante le recenti intrusioni, le organizzazioni possono essere meglio preparate e prendere decisioni intelligenti in materia di sicurezza.

Nel 2021, gli esperti Mandiant hanno osservato l'utilizzo da parte degli aggressori del 70% di tecniche MITRE ATT&CK e del 46% di sottotecniche. Rispetto al 2020, ciò rappresenta un aumento dell'11% delle tecniche osservate e un aumento del 92% delle sottotecniche. Sebbene ciò sia indicativo del fatto che gli aggressori utilizzano una più ampia varietà di tecniche per portare avanti le intrusioni, gli esperti di Mandiant ritengono che questo aumento sia dovuto in parte a una classificazione più solida e a una categorizzazione sistematica dei dati sulle minacce, implementata nel 2021.

Nel 2021, il 43% delle tecniche osservate (il 30% di tutte le tecniche) è stato rilevato in oltre il 5% delle intrusioni rispetto al 37% delle tecniche osservate nel 2020 (il 23% di tutte le tecniche nel 2020). Gli esperti Mandiant consigliano di dare priorità all'implementazione di misure di sicurezza per la protezione contro le tecniche più comunemente utilizzate rispetto a quelle con una minore diffusione.

MITRE ATT&CK® è una base di conoscenza accessibile a livello globale, riguardante le tattiche e le tecniche degli aggressori basate su osservazioni del mondo reale. La base di conoscenza ATT&CK viene utilizzata come fondamento per lo sviluppo di specifici modelli e metodi di aggressione nel settore privato e governativo e nella comunità operante nel campo dei prodotti e servizi correlati alla sicurezza informatica.

Tecniche MITRE ATT&CK più frequentemente utilizzate, 2021



In oltre la metà delle intrusioni esaminate nel 2021, Mandiant ha osservato che gli aggressori hanno utilizzato l'offuscamento, come crittografia o codifica, sui file o sulle informazioni, allo scopo di renderne più difficile il rilevamento e la successiva analisi (T1027).

Gli aggressori hanno inoltre utilizzato regolarmente un interprete di comandi o di script per ulteriori intrusioni (T1059) e il 65% di questi casi (il 29% di tutte le intrusioni) ha comportato l'uso di PowerShell (T1059.001).

Nel 37% delle indagini, l'aggressore ha comunicato utilizzando protocolli a livello delle applicazioni (T1071) e l'87% di questi (il 32% di tutte le indagini) ha utilizzato specificamente protocolli Web come HTTP e HTTPS.

Gli esperti Mandiant hanno osservato che gli aggressori eseguono azioni di scoperta di informazioni di sistema (T1082) nel 32% delle indagini e di informazioni su file o directory (T1083), sempre nel 32% delle indagini. In modo analogo, nel 32% delle indagini gli aggressori hanno rimosso gli indicatori su un host (T1070) e l'85% di questi (il 27% di tutte le indagini) ha comportato l'eliminazione di file.

Come nel 2020, gli aggressori hanno dimostrato la volontà di approfittare di ciò che è disponibile nell'ambiente vittima per effettuare ulteriori intrusioni nel 2021. Questo è particolarmente evidente dalla frequenza con cui gli aggressori hanno utilizzato i protocolli Web, PowerShell, i servizi di sistema e desktop da remoto. Le organizzazioni devono bilanciare la comodità e l'accessibilità delle tecnologie comuni con la sicurezza degli ambienti.

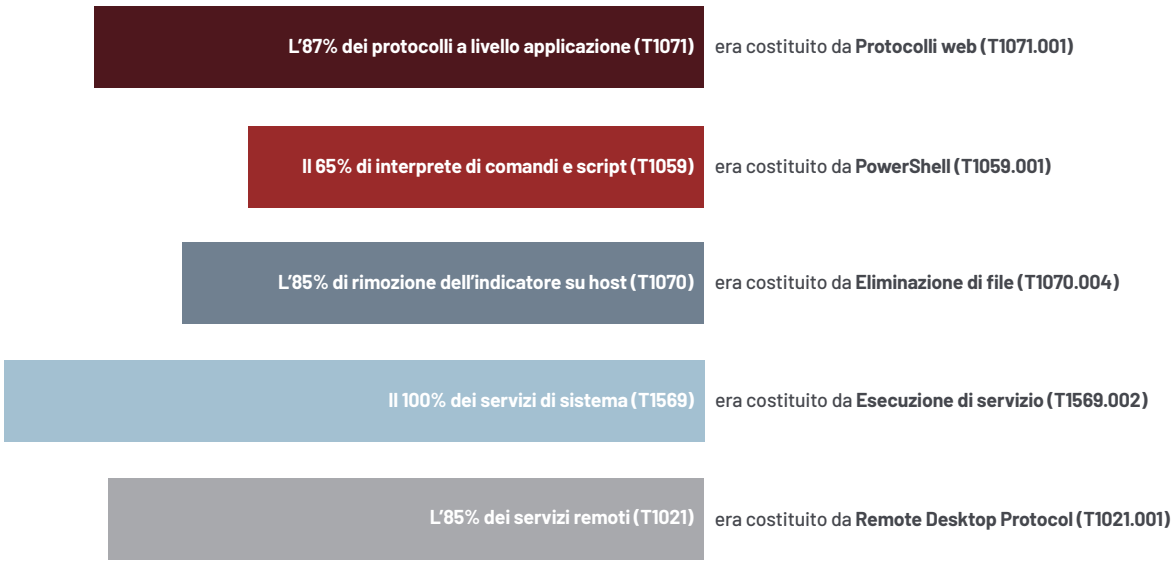
Le principali 10 tecniche osservate più frequentemente

1.	T1027: offuscamento di informazioni o file	51,4%
2.	T1059: interprete di comandi e script	44,9%
3.	T1071: protocollo a livello applicazione	36,8%
4.	T1082: scoperta delle informazioni di sistema	31,8%
5.	T1083: scoperta di file e directory	31,7%
6.	T1070: rimozione di indicatori sull'host	31,7%
7.	T1055: iniezione in un processo	28,5%
8.	T1021: servizi remoti	27,4%
9.	T1497: virtualizzazione/evasione sandbox	26,9%
10.	T1105: trasferimento di strumenti di ingresso	26,5%
	T1569: servizi di sistema	26,5%

Le principali 5 tecniche osservate più frequentemente

1.	T1071.001: protocolli Web	32,0%
2.	T1059.001: PowerShell	29,4%
3.	T1070.004: eliminazione dei file	27,1%
4.	T1569.002: esecuzione del servizio	26,5%
5.	T1021.001: Remote Desktop Protocol	23,4%

Tecnologie più frequentemente prese di mira, 2021



TECNICHE MITRE ATT&CK CORRELATE AL CICLO DI VITA DI UN ATTACCO, 2021

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Il ciclo di vita Mandiant di un attacco è la sequenza prevedibile di eventi che gli aggressori informatici utilizzano per portare a termine i loro attacchi. Per ulteriori informazioni, vedere: https://www.mandiant.com/resources/targeted-attack-lifecycle

Ricognizione iniziale

Ricognizione

Scansione attiva	0,8%	T1595.002: analisi delle vulnerabilità	0,5%
		T1595.001: scansione dei blocchi IP	0,3%

Sviluppo risorse

T1588: acquisizione capacità	16,0%	T1588.003: certificati di firma del codice	15,5%
		T1588.004: certificati digitali	0,5%
T1608: funzionalità delle fasi	12,9%	T1608.003: installazione di certificato digitale	9,2%
		T1608.005: obiettivo collegamento	3,5%
		T1608.004: obiettivo drive-by	0,2%
		T1608.001: caricamento del malware	0,2%
		T1608.002: caricamento di uno strumento	0,2%
T1583: acquisizione infrastruttura	9,4%	T1583.003: Virtual Private Server	9,4%
T1584: compromissione infrastruttura	3,4%		
T1587: sviluppo capacità	1,7%	T1587.003: certificati digitali	0,9%
		T1587.002: certificati di firma del codice	0,8%

Compromissione iniziale

Accesso iniziale

T1190: sfruttamento di applicazioni pubbliche	25,8%		
T1195: compromissione supply chain	11,1%	T1195.002: compromissione supply chain software	11,1%
T1133: servizi remoti esterni	8,8%		
T1566: phishing	8,6%	T1566.001: allegati spearphishing	4,3%
		T1566.002: link spearphishing	3,5%
T1078: account validi	6,3%		
T1189: compromissione drive-by	4,3%		
T1199: rapporti di fiducia	0,6%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Consolidamento di una base di partenza

Persistenza

T1053: attività/lavoro pianificato	15,8%	T1053.005: attività pianificata	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1505: componente software del server	14,0%	T1505.003: Web shell	14,0%
		T1505.004: componenti IIS	0,5%
T1543: creazione o modifica del processo di sistema	13,1%	T1543.003: servizio Windows	12,8%
		T1543.002: servizio Systemd	0,5%
T1133: servizi remoti esterni	8,8%		
T1098: manipolazione di account	8,3%	T1098.001: credenziali aggiuntive per il cloud	0,6%
		T1098.002: autorizzazioni delegato email Exchange	0,6%
		T1098.004: chiavi autorizzate SSH	0,6%
T1547: esecuzione avvio automatico all'avvio o all'accesso	6,9%	T1547.001: chiave di avvio del registro/cartella di avvio	5,5%
		T1547.009: modifica di collegamento rapido	1,4%
		T1547.004: DLL Helper Winlogon	0,6%
		T1547.006: moduli ed estensione del kernel	0,2%
T1136: creazione di account	6,3%	T1136.001: account locale	1,5%
		T1136.002: account dominio	0,8%
		T1136.003: account cloud	0,5%
T1574: compromissione flusso di esecuzione	4,2%	Lore T1574.011: vulnerabilità autorizzazioni registro dei servizi	3,4%
		T1574.002: caricamento laterale DLL	0,9%
		T1574.001: compromissione ordine di ricerca DLL	0,3%
		T1574.008: intercettazione percorso tramite compromissione ordine di ricerca	0,2%
T1546: esecuzione innescata da evento	2,8%	T1546.003: Windows Management Instrumentation – Sottoscrizione all'evento	1,4%
		T1546.008: caratteristiche dell'accessibilità	0,9%
		T1546.007: DLL helper Netsh	0,3%
		T1546.010: DLL AppInit	0,2%
		T1546.001: modifica all'associazione file predefinita	0,2%
		T1546.015: assunzione del controllo oggetto componente	0,2%
		T1546.012: aggiunta di opzioni di esecuzione di file immagine	0,2%
		T1546.002: screensaver	0,2%
T1197: attività BITS	0,8%		
T1037: script di inizializzazione dell'avvio o dell'accesso	0,5%	T1037.001: script di accesso (Windows)	0,2%
		T1037.003: script di accesso alla rete	0,2%
		T1037.004: script RC	0,2%
T1556: modifica del processo di autenticazione	0,3%	T1556.003: moduli di autenticazione collegabili	0,3%
T1554: compromissione binario software client	0,2%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Aumento dei privilegi

Escalation dei privilegi

T1055: iniezione in un processo	28,5%	T1055.003: compromissione esecuzione thread	2,8%
		T1055.001: aggiunta di una libreria di collegamento dinamico	1,1%
		T1055.004: chiamata di procedura asincrona	0,9%
		T1055.012: hollowing processo	0,8%
		T1055.002: aggiunta eseguibile portabile	0,2%
T1053: attività/lavoro pianificato	15,8%	T1053.005: attività pianificata	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1543: creazione o modifica del processo di sistema	13,1%	T1543.003: servizio Windows	12,8%
		T1543.002: servizio Systemd	0,5%
T1134: manipolazione token accesso	12,2%	T1134.001: impersonificazione/furto di token	6,3%
		T1134.002: creazione di processo con token	0,2%
T1547: esecuzione avvio automatico all'avvio o all'accesso	6,9%	T1547.001: chiave di avvio del registro/cartella di avvio	5,5%
		T1547.009: modifica di collegamento rapido	1,4%
		T1547.004: DLL Helper Winlogon	0,6%
		T1547.006: moduli ed estensione del kernel	0,2%
T1078: account validi	6,3%		
T1574: compromissione flusso di esecuzione	4,2%	T1574.011: vulnerabilità autorizzazioni registro dei servizi	3,4%
		T1574.002: caricamento laterale DLL	0,9%
		T1574.001: compromissione ordine di ricerca DLL	0,3%
		T1574.008: intercettazione percorso tramite compromissione ordine di ricerca	0,2%
T1546: esecuzione innescata da evento	2,8%	T1546.003: Windows Management Instrumentation – Sottoscrizione all'evento	1,4%
		T1546.008: caratteristiche dell'accessibilità	0,9%
		T1546.007: DLL helper Netsh	0,3%
		T1546.010: DLL AppInit	0,2%
		T1546.001: modifica all'associazione file predefinita	0,2%
		T1546.015: assunzione del controllo oggetto componente	0,2%
		T1546.012: aggiunta di opzioni di esecuzione di file immagine	0,2%
		T1546.002: screensaver	0,2%
T1548: abuso del meccanismo di controllo elevazione	2,2%	T1548.002: bypass controllo account utente	2,0%
		T1548.001: Setuid e Setgid	0,2%
T1484: modifica criteri dominio	0,8%	T1484.001: modifica criteri gruppo	0,8%
T1037: script di inizializzazione dell'avvio o dell'accesso	0,5%	T1037.001: script di accesso (Windows)	0,2%
		T1037.003: script di accesso alla rete	0,2%
		T1037.004: script RC	0,2%
T1068: sfruttamento dell'aumento dei privilegi	0,3%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Ricognizione interna

Scoperta

T1082: scoperta delle informazioni di sistema	31,8%		
T1083: scoperta di file e directory	31,7%		
T1497: virtualizzazione/evasione sandbox	26,9%	T1497.001: controlli di sistema	17,7%
		T1497.003: evasione basata sul tempo	3,4%
T1012: registro query	21,1%		
T1033: scoperta proprietario/utente del sistema	19,1%		
T1057: scoperta del processo	18,9%		
T1016: scoperta configurazione rete di sistema	16,9%	T1016.001: scoperta connessione Internet	0,6%
T1518: scoperta del software	16,8%	T1518.001: scoperta del software di sicurezza	0,3%
T1087: scoperta account	13,7%	T1087.002: account dominio	2.3%
		T1087.001: account locale	1,4%
		T1087.004: account cloud	0,2%
		T1087.003: account email	0,2%
T1482: scoperta dominio affidabile	8,2%		
T1069: scoperta autorizzazione gruppi	8,2%	T1069.002: gruppi domini	2,0%
		T1069.001: gruppi locali	1,1%
		T1069.003: gruppi cloud	0,2%
T1007: scoperta servizio di sistema	8,0%		
T1010: scoperta applicazione Window	6,5%		
T1135: scoperta condivisione di rete	6,2%		
T1049: scoperta connessioni di rete del sistema	6,2%		
T1614: scoperta posizione del sistema	3,8%	T1614.001: scoperta lingua del sistema	3,8%
T1018: scoperta sistema remoto	2,6%		
T1046: scansione servizi di rete	2,0%		
T1580: scoperta infrastruttura cloud	0,8%		
T1124: scoperta ora del sistema	0,6%		
T1040: analisi dei parametri di rete	0,3%		
T1201: scoperta criteri password	0,3%		
T1538: dashboard servizi cloud	0,2%		
T1526: scoperta servizi cloud	0,2%		
T1619: scoperta oggetto di storage nel cloud	0,2%		
T1120: scoperta dispositivo periferico	0,2%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Spostamento laterale

Spostamento laterale

T1021: servizi remoti	27,4%	T1021.001: Remote Desktop Protocol	23,4%
		T1021.004: SSH	4,8%
		T1021.002: condivisioni amministrative SMB/Windows	4,0%
		T1021.005: VNC (Virtual Network Computing)	0,5%
		T1021.006: gestione remota Windows	0,2%
T1550: utilizzo materiale di autenticazione alternativo	0,8%	T1550.002: superamento hash	0,5%
		T1550.001: token di accesso alle applicazioni	0,2%
		T1550.003: superamento ticket	0,2%
T1570: trasferimento strumenti laterale	0,6%		
T1534: spearphishing interno	0,5%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Mantenimento della presenza

Persistenza

T1053: attività/lavoro pianificato	15,8%	T1053.005: attività pianificata	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1505: componente software del server	14,0%	T1505.003: Web shell	14,0%
		T1505.004: componenti IIS	0,5%
T1543: creazione o modifica del processo di sistema	13,1%	T1543.003: servizio Windows	12,8%
		T1543.002: servizio Systemd	0,5%
T1133: servizi remoti esterni	8,8%		
T1098: manipolazione di account	8,3%	T1098.001: credenziali aggiuntive per il cloud	0,6%
		T1098.002: autorizzazioni delegato email Exchange	0,6%
		T1098.004: chiavi autorizzate SSH	0,6%
T1547: esecuzione avvio automatico all'avvio o all'accesso	6,9%	T1547.001: chiave di avvio del registro/cartella di avvio	5,5%
		T1547.009: modifica di collegamento rapido	1,4%
		T1547.004: DLL Helper Winlogon	0,6%
		T1547.006: moduli ed estensione del kernel	0,2%
T1136: creazione di account	6,3%	T1136.001: account locale	1,5%
		T1136.002: account dominio	0,8%
		T1136.003: account cloud	0,5%
T1574: compromissione flusso di esecuzione	4,2%	T1574.011: vulnerabilità autorizzazioni registro dei servizi	3,4%
		T1574.002: caricamento laterale DLL	0,9%
		T1574.001: compromissione ordine di ricerca DLL	0,3%
		T1574.008: intercettazione percorso tramite compromissione ordine di ricerca	0,2%
T1546: esecuzione innescata da evento	2,8%	T1546.003: Windows Management Instrumentation – Sottoscrizione all'evento	1,4%
		T1546.008: caratteristiche dell'accessibilità	0,9%
		T1546.007: DLL helper Netsh	0,3%
		T1546.010: DLL AppInit	0,2%
		T1546.001: modifica all'associazione file predefinita	0,2%
		T1546.015: assunzione del controllo oggetto componente	0,2%
		T1546.012: aggiunta di opzioni di esecuzione di file immagine	0,2%
		T1546.002: screensaver	0,2%
T1197: attività BITS	0,8%		
T1037: script di inizializzazione dell'avvio o dell'accesso	0,5%	T1037.001: script di accesso (Windows)	0,2%
		T1037.003: script di accesso alla rete	0,2%
		T1037.004: script RC	0,2%
T1556: modifica del processo di autenticazione	0,3%	T1556.003: moduli di autenticazione collegabili	0,3%
T1554: compromissione binario software client	0,2%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Completamento missione

Raccolta

T1560: archiviazione dati raccolti	13,8%	T1560.001: archiviazione tramite utility	4,0%
		T1560.002: archiviazione tramite library	1,1%
T1056: acquisizione input	7,5%	T1056.001: keylogging	7,5%
T1213: dati da archivi di informazioni	6,9%	T1213.003: repository codice	1,1%
		T1213.002: Sharepoint	1,1%
		T1213.001: Confluence	0,3%
T1074: staging dei dati	4,6%	T1074.001: staging dei dati locali	3,8%
		T1074.002: staging dei dati remoti	1,5%
T1115: dati clipboard	4,3%		
T1113: acquisizione dello schermo	3,8%		
T1114: raccolta email	2,0%	T1114.002: raccolta email remota	1,1%
		T1114.001: raccolta email locale	0,3%
		T1114.003: regola inoltro email	0,2%
T1039: dati da unità condivisa di rete	1,1%		
T1530: dati da oggetto cloud storage	0,9%		
T1005: dati dal sistema locale	0,5%		
T1119: raccolta automatizzata	0,2%		
T1602: dati dal repository di configurazione	0,2%	T1602.002: dump configurazione dispositivo di rete	0,2%

Estrapolazione

T1567: esfiltrazione da servizi Web	3,1%	T1567.002: esfiltrazione nello storage cloud	0,9%
		T1567.001: esfiltrazione nel repository di codice	0,2%
T1020: esfiltrazione automatizzata	1,1%		
T1041: esfiltrazione su canale C2	0,6%		
T1030: limiti della dimensione di trasferimento dei dati	0,2%		
T1048: esfiltrazione su un protocollo alternativo	0,2%		

Impatto

T1486: dati crittografati per l'impatto	22,6%		
T1489: blocco del servizio	11,5%		
T1529: arresto/riavvio del sistema	4,9%		
T1490: blocco recupero sistema	3,2%		
T1496: compromissione risorse	3,2%		
T1485: distruzione di dati	2,8%		
T1565: manipolazione di dati	0,5%	T1565.001: manipolazione di dati memorizzati	0,5%
T1531: rimozione accesso account	0,3%		
T1491: defacement	0,2%	T1491.002: defacement esterno	0,2%
T1561: cancellazione di disco	0,2%	T1561.002: cancellazione di struttura del disco	0,2%

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Durante il ciclo di vita

Accesso alle credenziali

T1003: dumping delle credenziali OS	9,8%	T1003.001: memoria LSASS	4,3%
		T1003.003: NTDS	3,7%
		T1003.002: Sicurezza account manager	1,4%
		T1003.008: /etc/passwd e /etc/shadow	1,2%
		T1003.006: DCSync	0,8%
		T1003.004: segreti LSA	0,2%
T1056: acquisizione input	7,5%	T1056.001: keylogging	7,5%
T1552: credenziali non protette	4,0%	T1552.004: chiavi private	1,4%
		T1552.002: credenziali nel registro	1,1%
		T1552.001: credenziali nei file	0,6%
		T1552.006: preferenze criteri dei gruppi	0,6%
		T1552.003: cronologia bash	0,5%
		T1552.005: API metadati istanza cloud	0,3%
T1558: furto o falsificazione ticket Kerberos	2.5%	T1558.003: Kerberoasting	2,0%
		T1558.004: AS-REP roasting	0,3%
		T1558.001: biglietto d'oro	0,2%
T1555: credenziali da password memorizzate	2,0%	T1555.003: credenziali da browser web	1,4%
		T1555.005: gestioni password	0,5%
		T1555.004: gestione credenziali Windows	0,2%
T1110: forza bruta	3,7%	T1110.001: identificazione password	1,2%
		T1110.003: password spray	0,9%
		T1110.004: stuffing delle credenziali	0,5%
T1111: intercettazione autenticazione a due fattori	1,1%		
T1539: furto cookie di sessione web	0,8%		
T1187: autenticazione forzata	0,5%		
T1556: modifica del processo di autenticazione	0,3%	T1556.003: moduli di autenticazione collegabili	0,3%
T1040: analisi dei parametri di rete	0,3%		
T1606: creazione di credenziali Web	0,2%	T1606.001: cookie Web	0,2%

Comandi e Controlli

T1071: protocollo a livello applicazione	36,8%	T1071.001: protocolli Web	32,0%
		T1071.004: DNS	8,2%
		T1071.002: protocolli trasferimento file	0,3%
T1105: trasferimento di strumenti di ingresso	26,5%		
T1573: canale crittografato	14,3%	T1573.002: crittografia asimmetrica	13,7%
		T1573.001: crittografia simmetrica	0,6%
T1095: protocollo non a livello applicazione	12,8%		
T1090: proxy	6,2%	T1090.003: proxy multi-hop	3,5%
		T1090.004: domain fronting	0,8%
		T1090.001: proxy interno	0,2%
T1572: protocollo di tunneling	4,5%		
T1568: risoluzione dinamica	3,4%	T1568.002: algoritmi generazione dominio	3,4%
T1219: software accesso remoto	1,4%		
T1102: servizi web	1,1%	T1102.001: Dead Drop Resolver	0,2%
T1132: codifica dei dati	0,8%	T1132.001: codifica standard	0,8%
T1001: offuscamento dati	0,5%	T1001.002: steganografia	0,2%
T1008: canali di fallback	0,2%		

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

Evasione di difesa

T1027: offuscamento di informazioni o file	51,4%	T1027.005: rimozione indicatore dagli strumenti	9,8%
		T1027.002: compressione dei software	5,4%
		T1027.003: steganografia	3,4%
		T1027.004: compilazione dopo la consegna	0,5%
T1070: rimozione di indicatori sull'host	31,7%	T1070.004: eliminazione dei file	27,1%
		T1070.006: indicatore data e ora	6,5%
		T1070.001: cancellazione registro eventi di Windows	3,7%
		T1070.005: rimozione connessione condivisione rete	1,7%
		T1070.002: cancellazione dei registri di sistema Linux o Mac	0,5%
		T1070.003: cancellazione cronologia comandi	0,3%
T1055: iniezione in un processo	28,5%	T1055.003: compromissione esecuzione thread	2,8%
		T1055.001: aggiunta di una libreria di collegamento dinamico	1,1%
		T1055.004: chiamata di procedura asincrona	0,9%
		T1055.012: hollowing processo	0,8%
		T1055.002: aggiunta eseguibile portabile	0,2%
T1497: virtualizzazione/evasione sandbox	26,9%	T1497.001: controlli di sistema	17,7%
		T1497.003: evasione basata sul tempo	3,4%
T1140: deoffuscare/decodificare file o informazioni	23,5%		
T1112: modifica registro	22,3%		
T1564: nascondere artefatti	20,2%	T1564.003: finestra nascosta	18,9%
		T1564.008: regole per nascondere le email	0,9%
		T1564.004: attributi file NTFS	0,3%
T1553: sovversione controlli affidabili	15,5%	T1553.002: firma codice	15,5%
T1620: caricamento codice reflective	13,5%		
T1562: indebolimento difese	13,4%	T1562.001: disabilitazione o modifica strumenti	9,1%
		T1562.004: disabilitazione o modifica firewall di sistema	5,7%
		T1562.003: compromissione accesso alla cronologia dei comandi	0,5%
		T1562.008: disabilitazione dei registri nel cloud	0,3%
		T1562.007: disabilitazione o modifica firewall su cloud	0,2%
T1134: manipolazione token accesso	12,2%	T1134.001: impersonificazione/furto di token	6,3%
		T1134.002: creazione di processo con token	0,2%
T1202: esecuzione indiretta del comando	8,2%		
T1078: account validi	6,3%		
T1218: esecuzione proxy binario firmato	5,4%	T1218.011: Rundll32	3,4%
		T1218.005: Mshta	0,6%
		T1218.010: Regsvr32	0,6%
		T1218.007: Msiexec	0,5%
		T1218.002: pannello di controllo	0,3%
		T1218.003: CMSTP	0,2%

Ciclo di vita di un attacco mirato

Framework MITRE ATT&CK

20,00%	100,00%
10,00%	19,99%
5,00%	9,99%
2,00%	4,99%
0,00%	1,99%

T1574: compromissione flusso di esecuzione	4,2%	T1574.011: vulnerabilità autorizzazioni registro dei servizi	3,4%
		T1574.002: caricamento laterale DLL	0,9%
		T1574.001: compromissione ordine di ricerca DLL	0,3%
		T1574.008: intercettazione percorso tramite compromissione ordine di ricerca	0,2%
T1480: esecuzione guardrail	3,7%	T1480.001: environmental keying	0,2%
T1036: mascheratura	3,2%	T1036.005: corrispondenza nome o sede legittima	0,6%
		T1036.007: estensione del file doppia	0,3%
		T1036.003: rinomina utility di sistema	0,3%
T1548: abuso del meccanismo di controllo elevazione	2,2%	T1548.002: bypass controllo account utente	2,0%
		T1548.001: Setuid e Setgid	0,2%
T1222: modifica delle autorizzazioni di file e directory	1,7%	T1222.001: Modifica delle autorizzazioni di file e directory Windows	0,6%
		T1222,002: modifica delle autorizzazioni di file e directory Linux e Mac	0,5%
T1197: attività BITS	0,8%		
T1484: modifica criteri dominio	0,8%	T1484.001: modifica criteri gruppo	0,8%
T1550: utilizzo materiale di autenticazione alternativo	0,8%	T1550.002: superamento hash	0,5%
		T1550.001: token di accesso alle applicazioni	0,2%
		T1550.003: superamento ticket	0,2%
T1127: esecuzione proxy con utility di sviluppatore affidabile	0,5%	T1127.001: MSBuild	0,5%
T1556: modifica del processo di autenticazione	0,3%	T1556.003: moduli di autenticazione collegabili	0,3%
T1578: modifica infrastruttura elaborazione cloud	0,3%	T1578.002: creazione istanza cloud	0,3%
		T1578.003: eliminazione istanza cloud	0,2%
T1014: rootkit	0,3%		

Esecuzione

T1059: interprete di comandi e script	44,9%	T1059.001: PowerShell	29,4%
		T1059.003: Command Shell di Windows	11,2%
		T1059.005: Visual Basic	4,0%
		T1059.006: Python	3,4%
		T1059.007: JavaScript	1,8%
		T1059.004: Shell Unix	1,5%
T1569: servizi di sistema	26,5%	T1569.002: esecuzione del servizio	26,5%
T1053: attività/lavoro pianificato	15,8%	T1053.005: attività pianificata	13,5%
		T1053.003: Cron	0,5%
		T1053.001: At (Linux)	0,2%
T1204: esecuzione dell'utente	5.8%	T1204.001: link dannosi	3,4%
		T1204.002: file dannosi	2.5%
T1047: Windows Management Instrumentation	4,0%		
T1203: sfruttamento esecuzione client	2,0%		
T1559: comunicazione tra processi	0,8%	T1559.001: modello oggetto componente	0,5%
T1129: modelli condivisi	0,6%		

CONCLUSIONI

Il panorama delle minacce informatiche è vasto e profondo ed è continuamente influenzato dal mondo che ci circonda. Quando è iniziata la pandemia di COVID-19, abbiamo visto che assistenza sanitaria, ricerca e sviluppo venivano presi più di mira. Oggi, al momento della pubblicazione di *M-Trends 2022*, la situazione che si sta verificando in Ucraina dimostra quanto la geopolitica e il mondo informatico siano strettamente collegati.

Mandiant ha come missione quella di proteggere ogni azienda dalle minacce informatiche e renderla più consapevole sul suo assetto di sicurezza. Il report *M-Trends* annuale rappresenta uno sforzo significativo per portare avanti questa missione con l'utilizzo dei dati e degli insegnamenti tratti dalle nostre attività di risposta agli incidenti.

Il tempo di attesa mediano globale è ora di 21 giorni, in calo rispetto ai 24 giorni dello scorso anno, una tendenza al ribasso che ci piace vedere. Una tendenza invece poco gradita è il continuo ricorso al ransomware e all'estorsione di vario tipo. Con bassi rischi e barriere all'ingresso e alte ricompense, riteniamo che questa sia una minaccia continua che mette a rischio tutte le organizzazioni.

La preparazione, che sia attraverso il red team, gli esercizi di simulazione, la formazione o altre tecniche, è fondamentale non solo per il ransomware ma per tutti i tipi di attacchi. Anche principi solidi, come la gestione delle vulnerabilità e delle patch, i privilegi minimi e l'hardening, svolgono un ruolo importante nella costruzione di difese efficaci. Il nostro caso di studio sui coniatori di monete illustra il valore della registrazione e del followup degli avvisi, poiché l'indagine ha portato a minacce ancora più significative.

Al centro di qualsiasi capacità di difesa informatica c'è l'intelligence che la guida, e le migliori informazioni sulle minacce vengono raccolte direttamente dalle prime linee. Mandiant continuerà a condividere le conoscenze acquisite in prima linea in *M-Trends* per migliorare la nostra consapevolezza della sicurezza collettiva, la comprensione e le capacità al fine di garantire che le organizzazioni possano rimanere determinate nei loro sforzi di sicurezza informatica.

Per saperne di più, visita il sito www.mandiant.com/managed

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
Stati Uniti d'America +1.703.935.1700
+1.833.3MANDIANT (362.6342)
info@mandiant.com

Informazioni su Mandiant

Fin dal 2004, Mandiant® è stata un partner affidabile di aziende consapevoli della sicurezza. Oggi, le informazioni sulle minacce e l'esperienza di Mandiant, leader del settore, sono alla base di soluzioni dinamiche che aiutano le organizzazioni a sviluppare programmi più efficaci e a infondere fiducia nella loro preparazione informatica.

MANDIANT