

Bloccare gli attacchi sul
nascere: come Managed
XDR vince la battaglia
contro il ransomware





Le bande di criminali informatici specializzate in ransomware sono in costante evoluzione e adottano nuove tecnologie per migliorare tattiche e tecniche. Non appena è disponibile una nuova tecnologia, gli esperti di attacchi ransomware trovano il modo per utilizzarla a proprio vantaggio. Lo abbiamo visto nell'**attuale ondata di sviluppo dell'IA**: una tecnologia destinata a impieghi positivi viene rapidamente acquisita e utilizzata per scopi dolosi.

La nostra analisi di un campione globale di attacchi ransomware segnalati ha rivelato che tutti i settori sono presi di mira da questa tipologia di crimine informatico e che molti di loro hanno subito un aumento degli attacchi nel 2024 rispetto al 2023. Tra gli attacchi ransomware segnalati inclusi nel nostro campione, più di 1 su 5 (il 21%) ha colpito il settore sanitario nel 2023-2024, rispetto al 18% di un anno fa. Nello stesso periodo il numero di attacchi che hanno interessato i servizi finanziari è passato da meno dell'1% al 6%. È evidente che la minaccia, il suo impatto e i relativi costi stanno aumentando e non sono solo i nostri dati a dimostrarlo.

Il rapporto di Ransomware.org sullo stato del ransomware, **The State of Ransomware (2024)**, ha rivelato che “il totale dei pagamenti per ransomware è quasi raddoppiato raggiungendo la cifra di 1,1 miliardi di dollari nel 2023, superando la soglia di 1 miliardo di dollari per la prima volta in assoluto”.

In che modo gli attacchi ransomware violano le organizzazioni?

Esiste un gran numero di tattiche e punti di ingresso che gli aggressori usano per violare le organizzazioni con il ransomware. Molti aggressori provano più approcci contemporaneamente fino a quando non riescono a penetrare nella rete presa di mira. Alcune di queste tattiche sono:



Phishing, vishing, quishing, smishing

Nell'ordine, utilizzano account e-mail, chiamate e messaggi vocali, codici QR e messaggi SMS. Gli attacchi si basano sull'invio di link dannosi a un individuo designato, di solito al suo account o dispositivo aziendale. L'obiettivo è far sì che l'utente faccia clic su un link e inserisca le informazioni di accesso, che l'aggressore può quindi utilizzare per accedere alla rete o per indurre la vittima a scaricare allegati dannosi.



Sfruttamento di vulnerabilità software sconosciute o dovute a patch non applicate (zero-day)

A volte, un utente malintenzionato è in grado di identificare una vulnerabilità nel software prima ancora del fornitore o dell'organizzazione, cosa che gli consente di sfruttare la mancata applicazione di patch inserendo codice dannoso che lo aiuta a sottrarre i dati. Questo attacco è chiamato "zero-day". Le bande specializzate in ransomware analizzano inoltre attivamente le reti alla ricerca di vulnerabilità note alle quali non sono ancora state applicate patch e le selezionano per sferrare l'attacco.



Hardware infetto

Alcuni aggressori utilizzano metodi più tradizionali, come l'invio di hardware infetto a un'azienda, ad esempio chiavette USB con ransomware che poi si diffonde attraverso i file del bersaglio e li crittografa. L'aggressore chiederà quindi un riscatto per decrittografare i dati.



Attacchi alla supply chain

Gli attacchi alla catena di approvvigionamento prendono di mira un fornitore o un servizio esterni utilizzati da un'azienda e aggiungono codice dannoso al loro software. Quindi, quando il fornitore invia un aggiornamento, il malware si diffonde all'organizzazione presa di mira venendo a costituire un attacco ransomware indiretto.



Interni malintenzionati

Alcuni attacchi ransomware provengono dall'interno dell'organizzazione tramite individui comunemente noti come interni, o insider, malintenzionati. Si tratta di persone che sono state spinte all'azione da una banda di ransomware o che gestiscono personalmente operazioni di ransomware, e che utilizzano le proprie credenziali di accesso per violare l'azienda per cui lavorano.

Questi sono solo alcuni dei modi in cui gli esperti di attacchi ransomware possono violare un'organizzazione; gli aggressori sviluppano continuamente nuovi metodi. Un modo utile per spiegare l'approccio alla difesa di tutti questi punti di ingresso è confrontarlo con la protezione di un'abitazione. Una configurazione completa per la protezione della casa, con telecamere a circuito chiuso, allarmi antintrusione, serrature avanzate e avvisi automatici, è molto più sicura di un sistema basato solo sulla chiusura a chiave delle porte. Se al livello di sicurezza già in essere si associano rilevamento e risposta, oltre ai metodi di difesa più tradizionali, la protezione sarà molto migliore.



Le organizzazioni sono pronte per rispondere agli attacchi ransomware?

La capacità di rispondere a un attacco ransomware risiede nella maturità della strategia di risposta alle minacce di un'organizzazione. Poiché le capacità dei criminali informatici sono sempre più sofisticate, la strategia deve evolversi in linea con gli sviluppi delle tattiche dei malintenzionati. Il rapporto di Ransomware.org citato in precedenza ha rilevato che solo il 14% degli intervistati afferma di essere assolutamente pronto con piani di risposta testati. Circa il 35% delle organizzazioni ha dichiarato di avere una preparazione parziale con carenze in alcuni settori e il 15% ha ammesso la propria impreparazione. Con l'86% degli intervistati dichiaratamente impreparato, non c'è dubbio che una gran parte delle organizzazioni debba adottare nuove e più forti difese per proteggersi dal ransomware.

Presentazione di rilevamento e risposta estesi gestiti (Managed XDR)

Rafforzare i sistemi di rilevamento e risposta dell'organizzazione è un modo affidabile per aumentare l'efficacia della strategia di protezione dal ransomware già impiegata. Spesso le

organizzazioni non si rendono conto per mesi di avere subito una violazione, il che aumenta i danni e il tempo necessario per riprendersi dall'attacco.

Tempo generalmente necessario per la risoluzione

	Senza XDR	Con XDR
Risoluzione BEC tipica (solo gateway)	1-2 mesi	1-2 ore
Risoluzione dei furti di identità	3-4 settimane	1-2 ore
Risoluzione delle infezioni da malware	3-4 settimane	Circa 1 ora
Risoluzione delle minacce interne	3-6 mesi	Circa 4 ore
Risoluzione delle estorsioni senza XDR	Variabile	Meno di 24 ore

Ma gli addetti alla sicurezza di molte organizzazioni subiscono già la pressione di tempi molto stretti e di carichi di lavoro pesanti e non sono in grado di aggiungere ulteriori responsabilità alla lista sempre più lunga delle loro mansioni.

Un sondaggio del 2022 condotto da Cybersecurity Insiders, [The State of Extended Detection and Response](#), ha rilevato che per il 52% delle organizzazioni la mancanza di personale qualificato è il problema principale a livello di sicurezza informatica. La soluzione, secondo Ransomware.org: “Aumentare le capacità interne di risposta al ransomware con servizi esternalizzati e/o gestiti a cura di partner affidabili”. L’implementazione di una soluzione XDR gestita è un modo molto efficace per introdurre le funzionalità complete di rilevamento e risposta di cui le organizzazioni hanno bisogno per ampliare la struttura della sicurezza informatica già presente, soprattutto quando non dispongono di personale qualificato.

Managed XDR offre un unico archivio per dati di sicurezza e telemetria unitamente a capacità di analisi per interpretare tali dati e accelerare il rilevamento delle minacce. Managed XDR fornisce anche risposte automatiche agli incidenti sulla base di schemi e piani concordati in precedenza. Inoltre, i sistemi di rilevamento e risposta per reti raccolgono e controllano i registri

dei dispositivi di rete e analizzano il traffico in entrata, in uscita e in transito della rete aziendale.

Managed XDR prende i dati di sicurezza generati da ciascuna di queste fonti e da altre ancora. Successivamente gli analisti della sicurezza li interpretano, contrastano le minacce o forniscono alle organizzazioni linee guida pratiche per porvi rimedio, accelerando il rilevamento e velocizzando i tempi di risposta. Ciò consente di ottenere informazioni migliori e di separare le minacce reali dai falsi allarmi. Circa il 72% degli intervistati per il sondaggio di Cybersecurity Insiders concorda sul fatto che Managed XDR sia una piattaforma fondamentale estremamente importante.

Impatto di XDR sul miglioramento del livello di sicurezza

La parte di XDR relativa al rilevamento offre alle organizzazioni una maggiore visibilità olistica sullo stato della loro rete e su tutte le minacce che tentano di accedervi, che si tratti di ransomware o altro. È come la telecamera di sorveglianza dell'impianto antifurto di una casa: tutto ciò che accade nella proprietà è sotto costante osservazione. Questa "telecamera" analizza gli eventi con una precisione migliore e con capacità maggiori rispetto a un essere umano che verifica manualmente la presenza di minacce. XDR può anche bloccare minacce come indirizzi IP, domini e hash di file che identifica come dolosi, proprio come una serratura efficace può bloccare i ladri di appartamento.

L'automazione è una parte fondamentale di XDR che aiuta a velocizzare notevolmente la risposta agli incidenti. Come l'impianto antifurto di una casa, può inviare risposte e avvisi automatici per consentire una reazione rapida alle minacce per la sicurezza e informare le persone necessarie. Un altro vantaggio essenziale è

la semplificazione offerta: non sono necessarie molteplici soluzioni specifiche di fornitori diversi per il rilevamento delle minacce e la risposta quando si dispone di una soluzione XDR gestita. Inoltre, semplifica il reporting sia per l'analisi dei dati che per la conformità, perché registra tutte le potenziali minacce, gli avvisi e le risposte automatiche con un sistema di reporting centralizzato, proprio come i registri cronologici degli eventi generati dagli impianti antifurto domestici. Maggiori informazioni sul funzionamento di XDR e sui vantaggi per le organizzazioni sono disponibili nel nostro eBook [XDR in breve: un approccio strategico alla gestione delle minacce](#).

Per saperne di più su come i servizi XDR gestiti possano rafforzare il livello di sicurezza informatica della tua organizzazione, visita il [nostro sito Web](#). Scoprirai anche come Barracuda possa accelerare il rilevamento e ridurre i tempi di risposta grazie a un servizio XDR gestito secondo la formula 24/7/365.

Informazioni su Barracuda

Barracuda si adopera per rendere il mondo più sicuro. Crediamo che tutte le aziende meritino l'accesso a soluzioni di sicurezza di livello enterprise cloud-first, che siano semplici da acquistare, implementare e utilizzare. Proteggiamo l'e-mail, le reti, i dati e le applicazioni con soluzioni innovative espandibili e adattabili lungo il percorso dei clienti. Centinaia di migliaia di organizzazioni in tutto il mondo si affidano a Barracuda per essere protette e supportate, in modo da potersi concentrare sulla propria attività e salire di livello. Ulteriori informazioni sono disponibili sul sito barracuda.com.

