Febbraio 2026

Rapporto sulle minacce

Report sulle minacce globali di Managed XDR

Come gli attaccanti prendono di mira le organizzazioni e le lacune nella sicurezza

Barracuda®
Your business, secured.

Sommario

Introduzione

Gli strumenti avanzati e gli esperti di Barracuda Managed XDR monitorano e proteggono le reti dei clienti 24 ore su 24, 365 giorni all'anno. Ogni minuto, la soluzione rileva e risponde a un avviso di sicurezza. Ogni 15 minuti, invia un avviso a un cliente e ogni 60 minuti blocca automaticamente una minaccia di alta gravità, come un dispositivo compromesso o un incidente di ransomware in corso.

Se non risolto, un singolo campanello d'allarme può rapidamente trasformarsi in un incidente diffuso che interrompe le operazioni, riduce la produttività, compromette i dati sensibili e danneggia la stabilità finanziaria e la reputazione del marchio. Nessuna organizzazione è immune; gli attaccanti prendono di mira aziende di ogni dimensione, in tutti i settori e le geografie.

Ciò che rende vulnerabili gli obiettivi può essere costituito da molte cose: lacune nella sicurezza, dispositivi non autorizzati, sistemi non aggiornati, disattenzioni, configurazioni errate e una mancanza di tempo e risorse per individuare l'intrusione, rimuovere gli attaccanti e chiudere saldamente la porta dietro di loro.

Lo scopo di questo rapporto è aiutare i professionisti IT e della sicurezza in organizzazioni con risorse limitate a comprendere meglio come gli attaccanti prendono di mira le potenziali vittime e i punti deboli della sicurezza che cercheranno di sfruttare. Forniamo esempi di incidenti reali e raccomandazioni su come rimanere al sicuro e resilienti dal punto di vista informatico.

In un mondo di minacce informatiche sempre più complesse ed elusive, le organizzazioni non affrontano la sfida da sole. Il tuo fornitore di sicurezza ha gli strumenti e le conoscenze per aiutarti a risolvere i problemi identificati in questo rapporto — e siamo con te in ogni fase del percorso.

I dati di supporto

I risultati dettagliati in questo rapporto si basano su Barracuda Managed XDR's un dataset unico di oltre due trilioni di eventi IT raccolti durante il 2025, quasi 600.000 avvisi di sicurezza e più di 300.000 endpoint protetti, firewall, server, risorse cloud e altro ancora. Circa 53.000 minacce di alta gravità sono state gestite dalla piattaforma di orchestrazione della sicurezza e risposta automatizzata (SOAR) di Barracuda Managed XDR.

Risultati principali

100%

degli incidenti di sicurezza hanno coinvolto almeno un endpoint non protetto o non autorizzato

96%

degli incidenti che coinvolgono il movimento laterale si sono conclusi con il rilascio di ransomware

66%

degli incidenti ha coinvolto la catena di fornitura o una terza parte (in aumento rispetto al 45% nel 2024)

3 ore

l'attacco ransomware più veloce, dalla violazione alla crittografia

90%

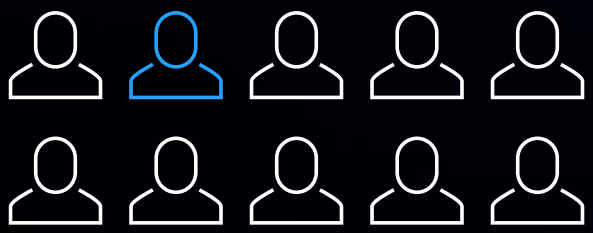
di incidenti ransomware hanno sfruttato i firewall

13 anni

la vulnerabilità più rilevata è un bug del 2013 nella crittografia obsoleta

1 su 10

le vulnerabilità rilevate hanno un exploit noto



Come gli attaccanti prendono di mira le organizzazioni

Le soluzioni efficaci di rilevamento e risposta estesa (XDR) sono progettate per intercettare le minacce in entrata nella fase più precoce della catena di attacco — il punto di compromissione iniziale e accesso. Barracuda Managed XDR non fa eccezione. Fornisce inoltre una visibilità aggiuntiva nelle fasi successive dell'attacco, inclusi il movimento laterale e l'impatto. Questa ampia capacità si riflette nel contenuto di questo rapporto.

In cima alla lista delle minacce più rilevate contro le organizzazioni negli ultimi 12 mesi ci sono gli attacchi che prendono di mira le identità e la sicurezza delle identità.

Questo include accessi insoliti o inattesi a un account utente. Si tratta di connessioni che non corrispondono al tipico comportamento dell'utente in termini di dispositivo, posizione o orario. Tali rilevamenti sono un forte indicatore di furto di credenziali e compromissione dell'account. Altri segnali di allarme sono i tentativi di connessione da una geolocalizzazione bloccata e la regola del 'viaggio impossibile', in cui un utente accede da una seconda posizione che non avrebbe mai potuto raggiungere nel tempo tra gli accessi.

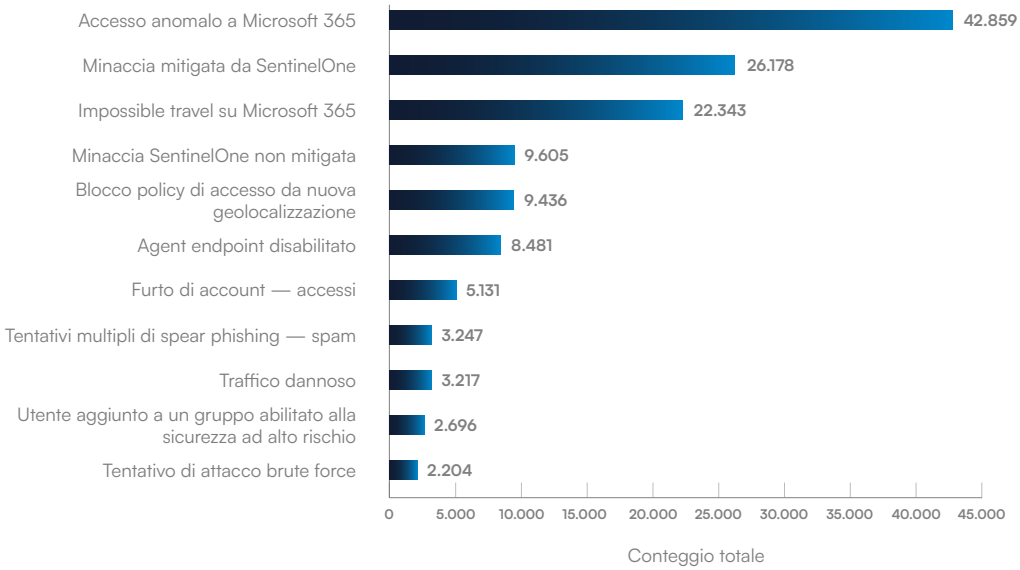


FIGURA 1

Principali rilevamenti di attacchi contro le organizzazioni

L'elenco delle principali rilevazioni include anche attività che potrebbero indicare che un account è stato compromesso e che gli attaccanti sono nella rete. I team di sicurezza devono indagare immediatamente su tali rilevazioni. Esse includono segnali che suggeriscono che qualcuno ha tentato di bypassare o disabilitare la protezione degli endpoint e notifiche che un utente è stato aggiunto a un gruppo sensibile alla sicurezza, il che potrebbe essere un attaccante che cerca di aumentare i propri privilegi.

Come gli attaccanti manomettono i diritti di privilegio una volta all'interno del sistema

L'escalation dei privilegi è cruciale per gli attaccanti perché trasforma un accesso limitato in un controllo amministrativo completo, consentendo loro di disabilitare le difese, muoversi lateralmente tra i sistemi e accedere a dati sensibili. Il risultato può essere un compromesso su larga scala e il rilascio di ransomware.

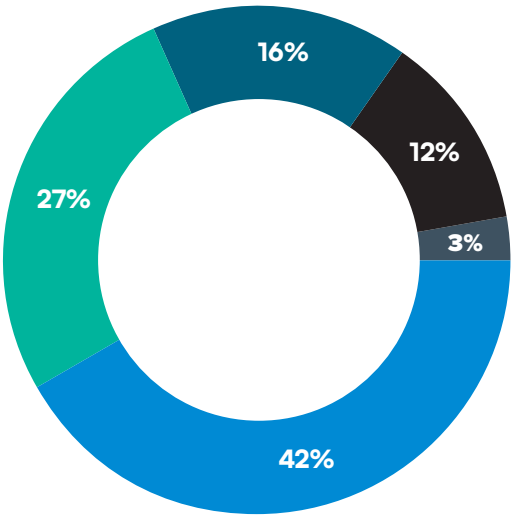


FIGURA 2

Come gli attaccanti manipolano i privilegi

- Windows — Aggiunto un utente a un gruppo con diritti di sicurezza ad alto rischio
- Windows — Rimosso un utente da un gruppo con diritti di sicurezza ad alto rischio
- Microsoft 365 — Aggiunto un utente come amministratore globale
- Microsoft 365 — Rimosso un utente come amministratore globale
- FortiGate Firewall — Aggiunto un utente come amministratore

Gli strumenti di sicurezza del firewall, Windows e Microsoft 365 di Barracuda Managed XDR hanno rilevato i seguenti comportamenti che indicano un tentativo di escalation dei privilegi:

Windows — ha aggiunto un utente a un gruppo con diritti di sicurezza ad alto rischio (rappresentando il 42% delle escalation di privilegi sospette)

- **Cosa significa:** Un utente è stato aggiunto a un gruppo con autorizzazioni avanzate (ad esempio, amministratori di dominio).
- **Gli aggressori possono utilizzarlo per:** Muoversi lateralmente, distribuire malware o sottrarre dati.
- **Come garantire la sicurezza:** Monitorare le modifiche di gruppo e gestire l'assegnazione di tutti i diritti di accesso privilegiati.

Windows — ha rimosso un utente da un gruppo con diritti di sicurezza ad alto rischio (27%)

- **Cosa significa:** Un utente è stato rimosso da un gruppo con privilegi elevati.
- **Gli aggressori possono utilizzarlo per:** Coprire le proprie tracce dopo l'escalation dei privilegi.
- **Come garantire la sicurezza:** Indagare sui motivi della rimozione e verificare se prima della rimozione si siano verificati casi di uso improprio.

Microsoft 365 — ha aggiunto un utente come amministratore globale (16%)

- **Cosa significa:** A qualcuno è stato concesso il massimo livello di accesso in Microsoft 365.
- **Gli aggressori possono utilizzarlo per:** Creare nuovi account, rubare dati o disabilitare la sicurezza.
- **Come garantire la sicurezza:** Rivedere le modifiche ai ruoli degli amministratori, applicare l'autenticazione a più fattori (MFA) e introdurre adeguati processi di revisione e approvazione.

Microsoft 365 — rimosso un utente come amministratore globale (12%)

- **Cosa significa:** Qualcuno ha perso i propri diritti di amministratore globale.
- **Gli aggressori possono utilizzarlo per:** Evitare di essere individuati rimuovendo gli account aggiunti.
- **Come garantire la sicurezza:** Verificare che la modifica sia stata autorizzata e controllare i registri di audit per individuare eventuali attività sospette o usi impropri.

FortiGate Firewall — aggiunto un utente come amministratore per il firewall (3%)

- **Cosa significa:** È stato creato un nuovo account amministratore sul firewall.
- **Gli aggressori possono utilizzarlo per:** Disabilitare le protezioni e aprire backdoor.
- **Come garantire la sicurezza:** Verificare la legittimità dell'account e applicare controlli amministrativi rigorosi.

Rapporto sull'incidente — L'allegato dannoso che ha portato a un RAT

Un Trojan di accesso remoto (RAT) è stato trovato sui sistemi di un cliente dopo che un dipendente ha scaricato inavvertitamente un file eseguibile dannoso. Il file ha immediatamente tentato di stabilire la persistenza: ha chiesto di registrarsi come servizio di Windows, il che gli avrebbe permesso di avviarsi automaticamente, funzionare in background e operare con accesso a livello di sistema in modo da poter controllare il sistema da remoto senza supporto. Ha anche tentato di installare lo strumento di gestione remota fidato ScreenConnect tramite PowerShell.

Nascondersi in bella vista

L'aggiunta e la rimozione di utenti dai gruppi di accesso privilegiato è un'attività IT legittima. La capacità degli attaccanti di nascondere comportamenti dannosi tra le normali attività e strumenti quotidiani è una delle sfide più grandi che i team di sicurezza devono affrontare oggi.

Questo approccio di vivere della terra (LOTL) è in aumento, con attori delle minacce che sfruttano strumenti e tecniche software legittimi per eludere il rilevamento. Fortunatamente, l'IA sta aiutando i sistemi di sicurezza avanzati a rilevare anomalie sottili in attività apparentemente innocue che possono essere investigate e mitigate.

Rapporto sull'incidente — Il ransomware Akira utilizza lo strumento di gestione remota della vittima contro di essa

Gli attaccanti hanno ottenuto l'accesso al controller di dominio (DC) e hanno installato il Datto RMM. La loro attività rispecchiava da vicino ciò che un agente di backup potrebbe legittimamente fare durante i lavori programmati, il che faceva sembrare tutto come normale attività IT.

Una parola sugli strumenti di accesso remoto e gestione (RMM)

Gli strumenti di accesso remoto sono un obiettivo crescente per gli attaccanti. Compromettere con successo uno strumento RMM offre agli attaccanti una quantità significativa di potere riducendo al contempo il rischio di essere rilevati, poiché gli RMM sono ampiamente utilizzati dalle organizzazioni.

Negli ultimi 12 mesi, Barracuda Managed XDR ha mitigato incidenti che coinvolgono l'abuso, tra gli altri, di SonicWall SSL-VPN (una popolare rete privata virtuale), ScreenConnect, RDP (il protocollo di desktop remoto), PsExec (uno strumento da riga di comando per eseguire programmi e comandi su computer remoti), AnyDesk e altri firewall VPN.

Per ridurre il rischio, i team di sicurezza devono implementare sistemi di rilevamento che cerchino specificamente l'abuso di RMM. Ad esempio, Barracuda Managed XDR ha sviluppato una regola di rilevamento che utilizza la telemetria dagli endpoint per identificare le richieste inviate da ScreenConnect a domini di primo livello (TLD) sospetti.

Combinazioni di bandiere rosse

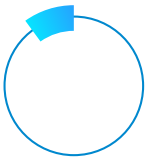
L'attività sospetta può essere identificata anche osservando il quadro generale. Un'analisi degli incidenti reali che hanno coinvolto Barracuda Managed XDR negli ultimi 12 mesi ha identificato le seguenti combinazioni comuni di strumenti/tecniche e comportamenti:

66%

dei casi che coinvolgono malware fileless hanno utilizzato PowerShell come metodo di esecuzione principale. PowerShell è uno strumento indipendente dalla piattaforma utilizzato per automatizzare le attività e gestire le configurazioni.

44%

di incidenti legati al firewall hanno coinvolto attacchi di password spraying, in cui gli attaccanti provano molte password comuni contro nomi utente rubati.



10%

delle violazioni della sicurezza dei server hanno comportato la cancellazione dei registri delle attività per coprire le tracce degli attaccanti.

96%

dei casi che coinvolgono movimenti laterali hanno portato al dispiegamento di ransomware.

90%

degli incidenti di ransomware hanno sfruttato i firewall attraverso una CVE (una vulnerabilità software classificata) o un account vulnerabile.

34%

degli incidenti hanno coinvolto l'ingegneria sociale che ha ingannato gli utenti inducendoli a scaricare file potenzialmente dannosi.

Per avere successo, gli attaccanti devono trovare e sfruttare le lacune nella sicurezza delle loro vittime designate. I dati di rilevamento e le informazioni sugli incidenti di Barracuda Managed XDR mettono in luce alcuni dei potenziali punti deboli che hanno lasciato i bersagli vulnerabili alle minacce informatiche nell'ultimo anno.

Come le organizzazioni si espongono

Principali vulnerabilità della sicurezza di rete

Metodi di crittografia inadeguati o obsoleti che non proteggono il traffico sensibile, così come la mancanza di una corretta convalida — o certificazione — dell'attività di rete possono essere utilizzati dagli attaccanti per portare avanti i loro attacchi.

Barracuda Managed XDR ha identificato i seguenti rischi per la sicurezza della rete nell'ultimo anno:

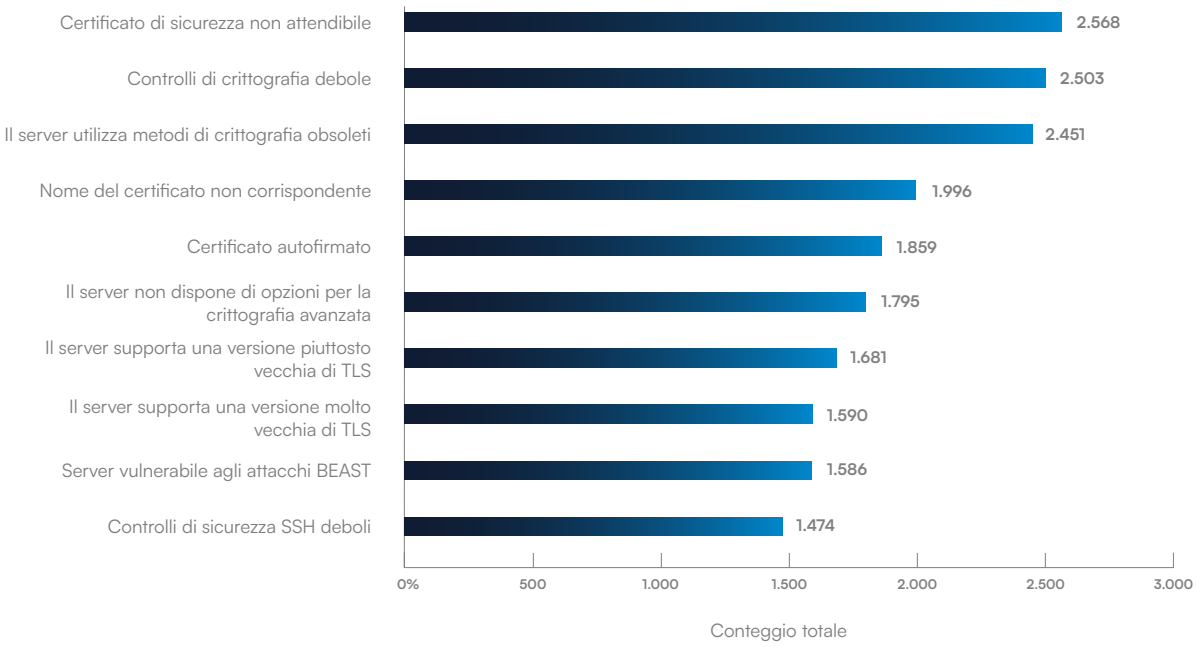


FIGURA 3

Principali vulnerabilità della sicurezza di rete

Certificato di sicurezza non affidabile

Cosa significa:

Il certificato presentato dal server non è emesso da un'Autorità di Certificazione (CA) attendibile.

Gli attaccanti possono usarlo per:

Impersonare un sito legittimo utilizzando un certificato falso, consentendo agli attaccanti di inserirsi nelle comunicazioni legittime per rubare dati, bypassare la sicurezza, iniettare contenuti dannosi e altro ancora.

Come rimanere al sicuro:

Utilizzare certificati da CA affidabili.

Per i team più tecnici: Implementare una corretta convalida dei certificati e abilitare il "certificate pinning" (in base al quale l'applicazione si fida solo di un certificato specifico quando si connette a un server). È inoltre importante verificare se il certificato di un'applicazione è stato revocato (utilizzando strumenti come CRL e OCSP) per evitare di fidarsi di certificati compromessi. Vedere: OWASP Certificato Convalida.

Controlli di crittografia deboli

Cosa significa:

Il server utilizza algoritmi deboli o lunghezze di chiave insufficienti per la crittografia.

Gli attaccanti possono usarlo per:

Forzare brutalmente o sfruttare le vulnerabilità per decrittografare dati sensibili come password e informazioni finanziarie. Il brute-forcing comporta il tentativo di molte combinazioni diverse di nome utente/password per vedere se una funziona.

Come rimanere al sicuro:

Imporre standard di crittografia robusti come AES-256, RSA-2048+.

Per i team più tecnici: Disattivare i codici di cifratura deboli e controllare regolarmente le configurazioni. Valutare l'implementazione della crittografia a curva ellittica (ECC), come ECDSA o ECDHE, per una maggiore sicurezza e prestazioni migliori (vedere: Raccomandazioni ECC del NIST). Utilizzare suite di cifratura Perfect Forward Secrecy (PFS) per proteggere le sessioni passate in caso di compromissione delle chiavi.

Il server utilizza metodi di crittografia obsoleti

Cosa significa:

Il server si basa su algoritmi ritirati come MD5, SHA-1 o RC4.

Gli attaccanti possono usarlo per:

Sfruttare vulnerabilità note per violare la crittografia o falsificare firme, portando a violazioni dei dati.

Come rimanere al sicuro:

Aggiorna a algoritmi moderni come SHA-256 o AES e segui le best practice del settore (ad esempio, le linee guida NIST sopra).

Per i team più tecnici: Rimuovere il supporto per gli algoritmi obsoleti (MD5, SHA-1, RC4) da tutte le configurazioni. Eseguire test con strumenti come SSL Labs per verificare che non siano abilitati algoritmi obsoleti. Vedi: SSL Labs Test.

Nome del certificato non corrispondente

Cosa significa:

Il nome di dominio non corrisponde al Common Name (CN) o al Subject Alternative Name (SAN) del certificato.

Gli attaccanti possono usarlo per:

Avvia attacchi di intercettazione reindirizzando il traffico a un server dannoso.

Come rimanere al sicuro:

Assicurati che i certificati corrispondano a tutti i domini/sottodomini in uso.

Per i team più tecnici: Utilizzate i campi SAN per i certificati multidominio. Automatizzate la gestione dei certificati per evitare discrepanze durante i rinnovi.

Certificato autofirmato

Cosa significa:

Il certificato è firmato dalla stessa entità che lo possiede, non da un'autorità di certificazione fidata.

Gli attaccanti possono usarlo per:

Rende più facile impersonare i server poiché chiunque può creare certificati autofirmati.

Come rimanere al sicuro:

Utilizzare certificati emessi da CA per i servizi rivolti al pubblico e limitare i certificati autofirmati ai sistemi interni.

Per i team più tecnici: Mantenete una CA privata per uso interno e distribuite il suo certificato root in modo sicuro. Monitorate la presenza di certificati autofirmati non autorizzati sulla vostra rete.

Il server non dispone di opzioni di crittografia robuste

Cosa significa:

Il server non offre suite di cifratura moderne e sicure.

Gli attaccanti possono usarlo per:

Forzare un downgrade a una crittografia più debole.

Come rimanere al sicuro:

Configura i server per supportare suite di cifratura robuste, come Transport Layer Security (TLS) 1.2/1.3 con AES-GCM.

Per i team più tecnici: Disattivare il supporto per opzioni di cifratura TLS deboli o non sicure come NULL o EXPORT, in modo che siano consentite solo connessioni forti, crittografate e autenticate. Aggiornare regolarmente il software del server per supportare i protocolli e le suite di cifratura più recenti.

Il server supporta versioni precedenti di TLS

Cosa significa:

La versione di TLS utilizzata è obsoleta e vulnerabile agli attacchi.

Gli attaccanti possono usarlo per:

Sfruttare le debolezze del protocollo per attacchi di intercettazione o downgrade che ingannano il sistema facendogli utilizzare un protocollo di sicurezza più vecchio e meno sicuro.

Come rimanere al sicuro:

Aggiorna la versione di TLS utilizzata.

Per i team più tecnici: Disabilitare TLS 1.0 e 1.1. Supporta solo TLS 1.2 e 1.3. Vedi: Mozilla Raccomandazioni TLS.

Il server supporta una versione molto vecchia di TLS

Cosa significa:

La versione di TLS in uso è obsoleta e insicura.

Gli attaccanti possono usarlo per:

Sfruttare le vulnerabilità note.

Come rimanere al sicuro:

Aggiorna la versione di TLS utilizzata.

Per i team più tecnici: Rimuovere completamente SSLv2, SSLv3 e le versioni TLS precedenti. Utilizzare strumenti automatizzati per verificare il supporto dei protocolli legacy.

Server vulnerabile ad attacco BEAST

Cosa significa:

Gli attacchi BEAST (Browser Exploit Against SSL/TLS) prendono di mira le versioni più vecchie di TLS che presentano debolezze nella loro crittografia basata su blocchi.

Gli attaccanti possono usarlo per:

Decrittografare HTTPS (Hypertext Transfer Protocol Secure) — una versione sicura del protocollo di comunicazione web di base) traffico ed espone dati riservati.

Come rimanere al sicuro:

Aggiorna all'ultima versione di TLS e utilizza suite di cifratura sicure.

Per i team più tecnici: Prendete in considerazione TLS 1.2+ con suite di cifratura AES-GCM o ChaCha20-Poly1305. Disattivate le cifrature in modalità CBC sulle versioni TLS precedenti.

Controlli di sicurezza SSH deboli

Cosa significa:

La configurazione SSH utilizza algoritmi deboli o protocolli obsoleti. SSH (Secure Shell) è un protocollo di rete sicuro utilizzato per accedere e controllare da remoto i computer su una rete non protetta, come internet.

Gli attaccanti possono usarlo per:

Forzare le credenziali o sfruttare chiavi deboli per ottenere accesso non autorizzato.

Come rimanere al sicuro:

Imponi algoritmi di scambio chiave forti, disabilita i protocolli SSH deboli, utilizza l'autenticazione basata su chiave e implementa strumenti specializzati di prevenzione delle intrusioni che proteggono i server dal brute forcing, come Fail2Ban o simili.

Per i team più tecnici: Utilizzare solo il protocollo SSH versione 2. Imporre lunghezze minime delle chiavi (ad esempio, RSA 4096, Ed25519). Disattivate l'autenticazione tramite password, se possibile, e utilizzate l'autenticazione basata su chiave. Limitate l'accesso SSH tramite IP e utilizzate regole firewall. Aggiornate regolarmente il software del server SSH. Vedere: SSH Security Best Practices.

Le principali vulnerabilità software CVE rilevate

I software obsoleti e privi di patch sono una calamita per le minacce informatiche. Secondo Barracuda Managed Vulnerability Security, queste sono le principali vulnerabilità software identificate nelle reti dei clienti nell'ultimo anno:

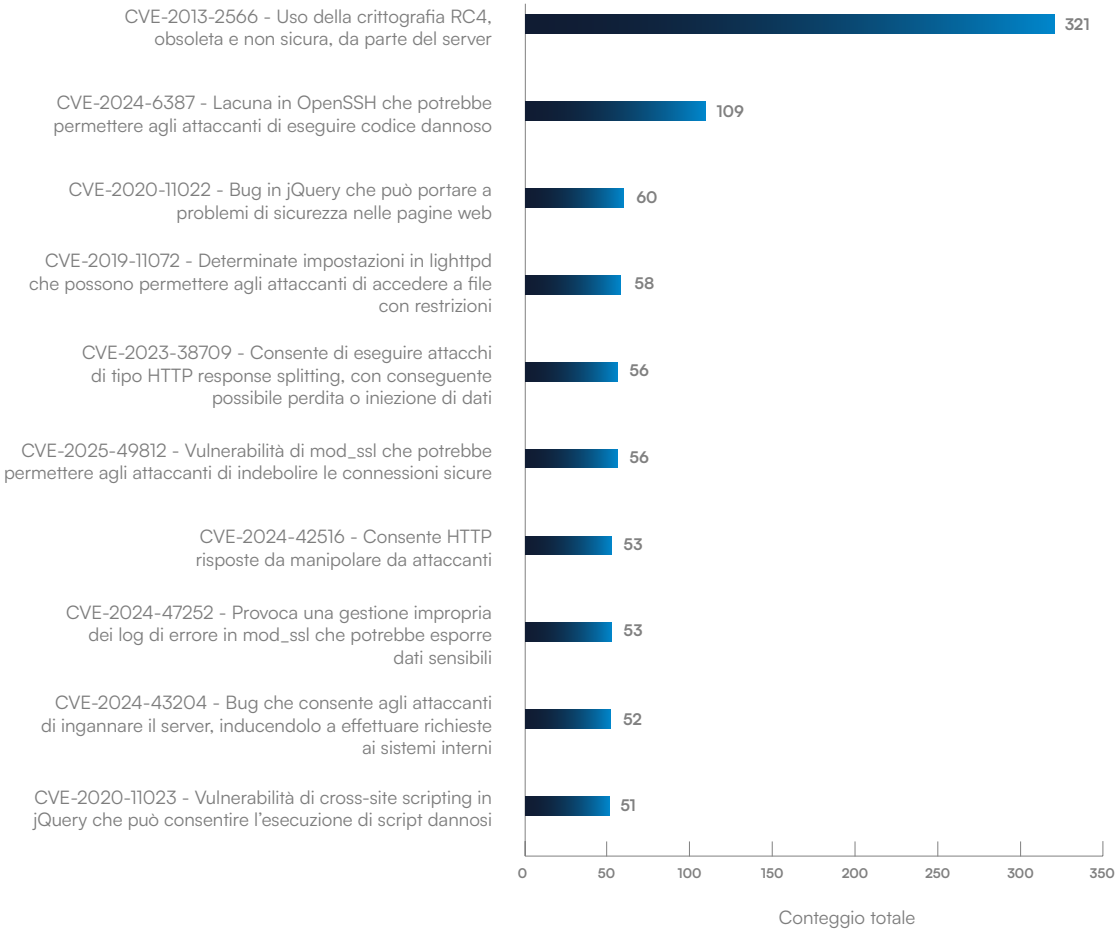


FIGURA 4

Principali vulnerabilità con CVE assegnato trovate nelle organizzazioni

La vulnerabilità più ampiamente rilevata è anche la più antica. CVE-2013-2566 esiste da quasi 13 anni e può ancora essere trovata in sistemi legacy come vecchi server, dispositivi embedded o applicazioni.

Questi sistemi possono essere in uso attivo, ma spesso sono inattivi e dimenticati. La prevalenza di questa vulnerabilità è un chiaro avvertimento sul rischio di esposizione dormiente. Prima viene corretta una vulnerabilità, minori sono le possibilità che venga trascurata.

Solo un CVE nell'elenco ha una valutazione di gravità critica, ma cinque sono designati ad alta gravità. Il punteggio medio di gravità di tutte le vulnerabilità rilevate negli ultimi 12 mesi è stato di 5,9.

CVE-2013-2566 — Il server si basa su crittografia RC4 vulnerabile e obsoleta

Gravità: **MEDIA**

Gli attaccanti possono usarlo per:

Sfruttare la crittografia debole per decrittografare i dati sensibili in testo semplice. RC4 è un tipo di cifrario di crittografia.

Come rimanere al sicuro:

Disabilita RC4 nelle configurazioni TLS (vedi sopra) e utilizza cifrari moderni come AES, TLS 1.2+.

CVE-2024-6387 — Un difetto in OpenSSH che potrebbe consentire agli attaccanti di eseguire codice dannoso

Gravità: **CRITICA**

Gli attaccanti possono usarlo per:

Ottieni il pieno controllo dei sistemi interessati da remoto. SSH è Secure Shell, un protocollo utilizzato per connettersi in modo sicuro a sistemi remoti su una rete non sicura come Internet, e OpenSSH è una versione gratuita e open-source.

Come rimanere al sicuro:

Applica immediatamente le ultime patch di OpenSSH e limita l'accesso SSH.

CVE-2020-11022 — Un bug in jQuery che può portare a problemi di sicurezza nelle pagine web

Gravità: **MEDIA**

Gli attaccanti possono usarlo per:

Iniettare script dannosi nelle pagine web e rubare sessioni e dati. jQuery è una libreria JavaScript che facilita la codifica per gli sviluppatori.

Come rimanere al sicuro:

Aggiorna all'ultima versione di jQuery e pulisci i dati prima che il tuo sistema li utilizzi.

CVE-2019-11072 — Alcune impostazioni nel server web lighttpd possono consentire agli attaccanti di accedere a file riservati

Gravità: **ALTA**

Gli attaccanti possono usarlo per:

Accedi a file riservati sul server, inclusi configurazioni o dati sensibili. Un server lighttpd è un server web open-source progettato per ambienti in cui la velocità è fondamentale.

Come rimanere al sicuro:

Aggiorna il server web lighttpd all'ultima versione e assicurati che le posizioni dei file fornite dagli utenti siano controllate e pulite per prevenire abusi.

CVE-2023-38709 — Consente agli attaccanti di dividere le risposte HTTP nei server web Apache vulnerabili, portando possibilmente a perdite di dati o iniezioni

Gravità: **ALTA**

Gli attaccanti possono usarlo per:

Aggiungi istruzioni false alle risposte web, inganna i sistemi per memorizzare dati dannosi o inietta codice dannoso nelle pagine web, compromettendo l'integrità dei dati e la sicurezza degli utenti.

Come rimanere al sicuro:

Aggiorna il server web Apache e assicurati che tutte le istruzioni o i dati di intestazione da browser a server siano correttamente controllati e puliti.

CVE-2025-49812 — Una vulnerabilità in mod_ssl che potrebbe consentire agli attaccanti di degradare le connessioni sicure

Gravità: **ALTA**

Gli attaccanti possono usarlo per:

Abbassare il livello di crittografia o intercettare il traffico ed esporre dati sensibili. mod_ssl è un modulo del server Apache HTTP che aggiunge supporto per la crittografia.

Come rimanere al sicuro:

Applica le ultime patch di Apache e applica configurazioni di crittografia TLS robuste.

CVE-2024-42516 — Una vulnerabilità di sicurezza che consente agli attaccanti di manipolare le risposte web HTTP inviate agli utenti

Gravità: **ALTA**

Gli attaccanti possono usarlo per:

Sfruttare le vulnerabilità nel modo in cui un sistema riceve, verifica e elabora i dati per iniettare contenuti dannosi o reindirizzamenti che possono portare a phishing, distribuzione di malware o furto di sessioni utente.

Come rimanere al sicuro:

Applica tempestivamente le patch del fornitore e applica intestazioni di sicurezza robuste.

CVE-2024-47252 — Risultato in gestione impropria dei log di errore in mod_ssl che potrebbe esporre dati sensibili

Gravità: **MEDIA**

Gli attaccanti possono usarlo per:

Inserire contenuti dannosi nei log che possono avvelenare i log e potenzialmente aumentare i privilegi.

Come rimanere al sicuro:

Aggiorna Apache e limita l'accesso ai log.

CVE-2024-43204 — Un bug che consente agli attaccanti di ingannare il server per effettuare richieste a sistemi interni

Gravità: **ALTA**

Gli attaccanti possono usarlo per:

Forzare un server a effettuare richieste ai sistemi interni, esponendo la rete interna.

Come rimanere al sicuro:

Applica patch ad Apache e convalida le configurazioni degli header

CVE-2020-11023 — Un difetto di cross-site scripting in jQuery che può consentire script dannosi

Gravità: **MEDIA**

Gli attaccanti possono usarlo per:

Inserire script dannosi.

Come rimanere al sicuro:

Aggiorna jQuery, pulisci gli input degli utenti e utilizza strumenti per bloccare il codice dannoso.

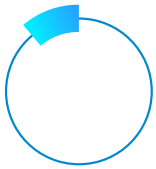
Risultati aggiuntivi da Barracuda Managed Vulnerability Security

4.146

Numero totale di vulnerabilità critiche rilevate.

2.525

Numero totale di vulnerabilità uniche identificate.



11%

Proporzione di vulnerabilità che hanno un exploit noto.

Rapporto sull'incidente — Firewall non aggiornato utilizzato nel tentativo di RansomHub

Gli attaccanti hanno sfruttato vulnerabilità non patchate in un firewall Fortinet. Hanno lanciato un'attività di forza bruta contro la rete di un cliente, ma sono stati bloccati. Un mese dopo, hanno tentato un accesso remoto (SSL VPN) ma sono stati bloccati di nuovo. Due giorni dopo, hanno fatto un terzo tentativo. Barracuda Managed XDR ha rilevato attività di PsExec (comando remoto) e ha trovato software dannoso sul controller di dominio primario e sul server di backup.

Configurazione errata: Incidenti che coinvolgono strumenti di sicurezza disabilitati accidentalmente o intenzionalmente

Gli strumenti di sicurezza che non sono stati configurati correttamente rappresentano un grande rischio per la sicurezza. Il pericolo può essere accentuato dal falso senso di sicurezza che deriva dall'avere lo strumento installato in primo luogo. Negli ultimi 12 mesi, Barracuda Managed XDR ha identificato funzionalità disabilitate che includevano agenti di protezione degli endpoint (che rappresentano il 94% delle rilevazioni di sicurezza disabilitate), MFA (3,62%), safe link (1,4%) e regole di allegati sicuri (0,6%).

Gli studi dimostrano che la maggior parte delle organizzazioni sta cercando di gestire troppi strumenti di sicurezza. Quando le risorse sono limitate, gli errori di configurazione possono facilmente insinuarsi. La migliore protezione è una piattaforma di sicurezza integrata con piena visibilità su impostazioni e configurazioni che può rapidamente e automaticamente segnalare le lacune che necessitano di correzione.

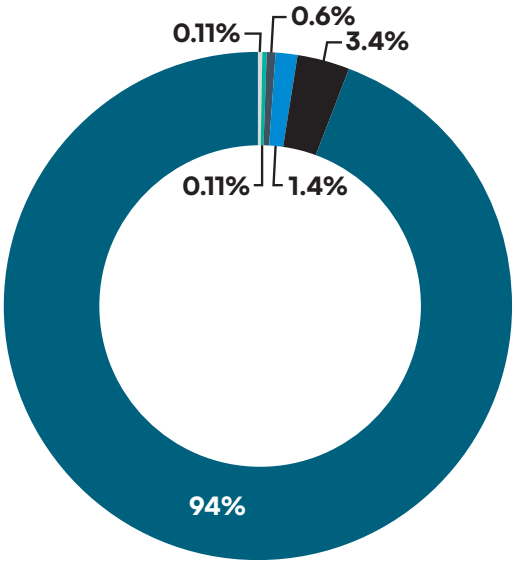


FIGURA 5

Funzionalità di sicurezza più comunemente disabilitate

- Agente SentinelOne Endpoint disabilitato
- MFA Microsoft 365 disabilitato
- Regola 'safe links' di Microsoft 365 ATP disabilitata
- Regola "allegati sicuri" di Microsoft Office ATP disabilitata
- MFA di Microsoft Azure disabilitato
- Google Workspace MFA disabilitato

100%

Proporzione di incidenti a cui Barracuda Managed XDR ha risposto che hanno coinvolto almeno un endpoint non protetto o non autorizzato

66%

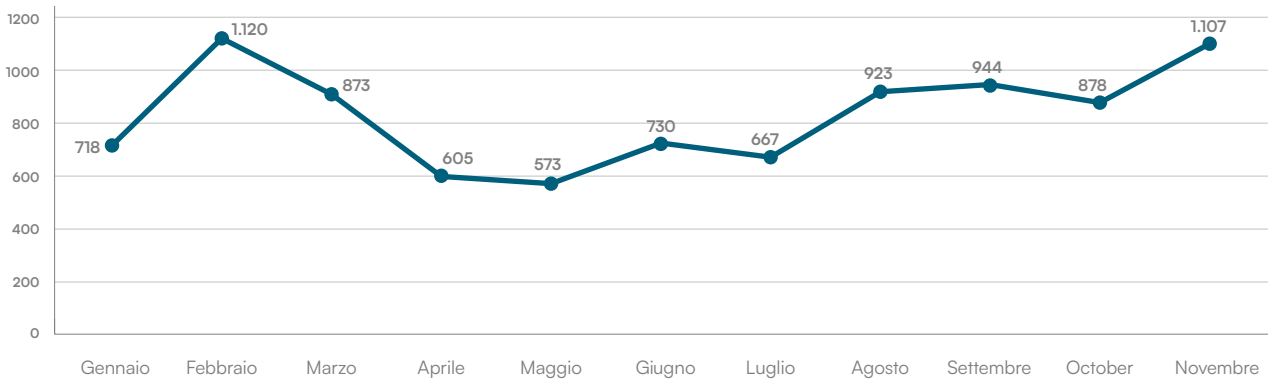
Proporzione di incidenti a cui Barracuda Managed XDR ha risposto che hanno coinvolto la catena di fornitura o una terza parte (in aumento rispetto al 45% nel 2024)

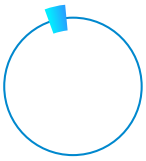
La minaccia persistente del ransomware

Negli ultimi 12 mesi, Barracuda Managed XDR ha identificato 13.514 indicatori che un attacco ransomware era in corso, inclusi strumenti, tecniche e comportamenti. A differenza degli anni precedenti, non ci sono più picchi o cali netti, ma un livello costantemente elevato di incidenti durante tutto l'anno.

FIGURA 6

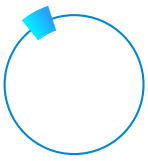
Incidenti correlati al ransomware nel 2025





1.5% a 5.6%

Proporzione di tutte le organizzazioni colpite da ransomware ogni mese nel 2024



5.1% a 10.9%

Proporzione di tutte le organizzazioni colpite da ransomware ogni mese nel 2025

Principali famiglie di ransomware incontrate nel 2025

Akira

- Akira è un gruppo di ransomware relativamente nuovo, noto per prendere di mira le organizzazioni con attacchi sofisticati. Spesso impiega tattiche di doppia estorsione, crittografando i dati e minacciando di divulgare informazioni sensibili a meno che non venga pagato un riscatto.
- **Tattiche**: Utilizzo di malware avanzato, attacchi mirati e furto di dati.

Qilin

- Qilin è un gruppo di ransomware che ha attirato l'attenzione per i suoi attacchi mirati alle infrastrutture critiche e alle organizzazioni aziendali.
- **Tattiche**: Doppia estorsione, sfruttamento delle vulnerabilità e utilizzo di malware per crittografare i dati.

RansomHub

- RansomHub è un'operazione ransomware che opera come ransomware-as-a-service (RaaS), consentendo agli affiliati di distribuire ransomware con il proprio marchio.
- **Tattiche**: Modello Ransomware-as-a-Service (RaaS), furto di dati ed estorsione.

Cactus

- Cactus è un gruppo di ransomware che è stato coinvolto in attacchi mirati, spesso richiedendo riscatti elevati.
- **Tattiche**: Crittografia dei dati, doppia estorsione e sfruttamento delle vulnerabilità.

Rapporto sull'incidente — Molteplici lacune di sicurezza espongono il bersaglio a Cactus

Gli obiettivi sono stati ingannati a scaricare file dannosi tramite chiamate Teams. Gli attaccanti hanno creato canali per emettere comandi da remoto, muoversi lateralmente e mantenere la persistenza. Attività pianificate dannose, modifiche al registro e DLL sideloading (quando un programma viene ingannato a caricare un file di codice condiviso falso e dannoso in modo che il codice dell'attaccante venga eseguito al posto di quello reale) hanno aiutato gli attaccanti a scalare i privilegi e a eludere il rilevamento. Il team Barracuda Managed XDR ha trovato dispositivi canaglia e più di 1.600 dispositivi non protetti sulla rete, permessi Microsoft Teams lassisti, distribuzioni vulnerabili del protocollo di desktop remoto (RDP) e secure shell, file non firmati e una mancanza di consapevolezza dei dipendenti.

Il ransomware si muove a velocità diverse

Secondo i dati di rilevamento e incidenti di Barracuda Managed XDR, i più veloci attacchi ransomware nel 2025 hanno impiegato solo poche ore dall'inizio alla fine, mentre i più lunghi hanno richiesto mesi.

Le intrusioni prolungate consentono il massimo danno poiché gli attaccanti hanno tempo per la ricognizione, l'esfiltrazione dei dati, il sabotaggio e altro ancora. Gli incidenti che si muovono a velocità fulminea possono essere più difficili da individuare e contenere prima che siano stati eseguiti e il danno sia fatto.

Le organizzazioni devono essere pronte per entrambi i tipi di attacchi e disporre di strumenti di sicurezza che siano sempre vigili.

La velocità del ransomware — 3 attori

Tempi stimati da incidenti nel mondo reale

Rapporto sull'incidente — XDR rileva il ransomware Akira che sfrutta un 'account fantasma' e un server non protetto

Gli attaccanti hanno violato la rete attraverso un account creato per un fornitore terzo e non disattivato quando se ne sono andati. Gli attaccanti hanno tentato di muoversi lateralmente e disabilitare la sicurezza degli endpoint, ma sono stati bloccati. Si sono spostati su un server non protetto, hanno aumentato i loro privilegi e lanciato il ransomware. Tutti i dispositivi impattati sono stati neutralizzati. Altri rischi trovati sulla rete target includevano dispositivi non protetti, un canale VPN aperto nel loro firewall e un MFA incoerente.

Conclusione: Come rimanere al sicuro in un mondo di minacce complesse

I team di sicurezza affrontano sfide crescenti. Con risorse limitate, devono proteggere un panorama in continua espansione di dispositivi, applicazioni, vulnerabilità critiche e strumenti di sicurezza frammentati, spesso senza la visibilità unificata necessaria per anticipare le minacce.

Tutto sta per diventare ancora più difficile poiché gli attaccanti iniziano a sfruttare l'IA agentica.

I sistemi di IA agentica automatizzeranno le fasi iniziali e ripetitive di un attacco, scansioneranno gli ambienti senza sosta, identificheranno configurazioni deboli e lanceranno exploit mirati in pochi minuti. Gli attori delle minacce che sfruttano agenti di IA saranno in grado di prendere decisioni, adattare strategie e correggere o riscrivere codice dannoso quando qualcosa fallisce o incontrano un ostacolo. Questo cambiamento aumenterà drasticamente la velocità, la scala e la coerenza degli attacchi.

Le organizzazioni necessitano di una strategia di sicurezza unificata che integri tecnologie di rilevamento avanzate, basate su IA, con un SOC completamente autonomo, completato da educazione degli utenti, risposta automatizzata alle minacce e una cultura della sicurezza resiliente.

Ci sono vittorie rapide, come quelle descritte in tutto questo rapporto. Includono l'autenticazione multifattoriale e i controlli di accesso coerenti, un approccio robusto alla gestione delle patch e alla protezione dei dati, e un training regolare per la sensibilizzazione sulla sicurezza informatica per i dipendenti.

Questo dovrebbe essere supportato da una piattaforma di sicurezza gestita e completa e da una soluzione XDR gestita 24/7 che integra la sicurezza di rete, endpoint, server, cloud ed e-mail, fornendo piena visibilità end-to-end e controllo di gestione supportato da un SOC completamente autonomo.

La sicurezza a lungo termine risiede nella resilienza informatica. Rilevamento e prevenzione sono i pilastri di qualsiasi strategia di sicurezza, ma di fronte a minacce sempre più complesse e elusive, la capacità di rispondere e riprendersi rapidamente dagli attacchi con un impatto minimo è fondamentale.

I risultati di questo rapporto si basano su dati di rilevamento da Barracuda Managed XDR, una piattaforma di visibilità estesa, rilevamento e risposta (XDR), supportata da un centro operativo di sicurezza (SOC) che offre ai clienti servizi di rilevamento delle minacce, analisi, risposta agli incidenti e mitigazione guidati da esseri umani e AI.

Barracuda Managed XDR fa parte di BarracudaONE, una piattaforma basata sull'intelligenza artificiale che protegge e-mail, dati, applicazioni e reti con soluzioni innovative e un dashboard centralizzato per massimizzare la protezione e rafforzare la resilienza informatica.

Informazioni su Barracuda

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