CROWDSTRIKE

Le principali tecniche di attacco al cloud

e come difendersi

Il cloud è una superficie di attacco in continua crescita ed evoluzione. Difendere questo ambiente dai proliferanti attacchi cloud richiede una conoscenza approfondita delle attività dei cybercriminali. Ecco le tre principali tendenze di attacco al cloud osservate da CrowdStrike e come difendersi.

I cybercriminali prendono sempre più spesso di mira il cloud

Gli ambienti cloud continuano a crescere:

41,4%
i cloud leader che affermano di stare aumentando il loro uso di servizi e prodotti basati sul cloud[1]

33,4%
chi progetta di migrare dal software aziendale legacy agli strumenti basati sul cloud[1]

32,8%
chi sta migrando i workload on premise al cloud[1]

E i cybercriminali se ne sono accorti.

Nel 2022, CrowdStrike ha osservato:

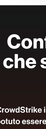
95%
di incremento nei casi di sfruttamento del cloud

3x
del numero di casi che coinvolgevano cybercriminali cloud conscious

71%
di attacchi privi di malware

Perché prendere di mira gli ambienti cloud?

Gli ambienti multi-cloud sono complessi e quindi
più difficili da proteggere



I processi di software delivery rapidi rendono le app cloud native più sensibili
a vulnerabilità e configurazioni errate

Gli ambienti cloud non autorizzati e shadow sono privi di
controlli di sicurezza e di vigilanza

I singoli prodotti di sicurezza lasciano dei punti ciechi
attraverso i quali gli avversari possono intrufolarsi inosservati

I cybercriminali sono esperti di cloud e affinano le loro tattiche per abusare dei servizi cloud e sfruttarne le vulnerabilità. Ecco le tre principali tecniche di attacco al cloud osservate dal team di threat intelligence di CrowdStrike nell'ultimo anno durante il monitoraggio di oltre 200 cybercriminali.

Movimento laterale nell'infrastruttura IT

I cybercriminali sfruttano sempre più spesso gli endpoint tradizionali per passare all'infrastruttura cloud e viceversa: l'infrastruttura cloud viene usata come gateway per accedere agli endpoint. Poiché hanno acquistato numerose soluzioni singole per far fronte all'ambiente on premise e, più recentemente, per affrontare gli ambienti cloud, raramente le organizzazioni godranno della visibilità necessaria per bloccare quest'attività.

Per bloccare il movimento laterale,
alle aziende serve una visibilità completa sull'intera infrastruttura IT, sia on premise che in cloud.

Configurazioni errate del cloud che sfociano in compromissioni

CrowdStrike indaga costantemente sulle compromissioni del cloud che avrebbero potuto essere rilevate o evitate prima se le impostazioni di sicurezza del cloud fossero state configurate correttamente. Le configurazioni errate non solo aumentano il rischio di compromissione, ma diventano sempre più preponderanti e problematiche man mano che le aziende espandono la loro infrastruttura cloud.

PRIMA
vulnerabilità negli ambienti cloud

60%
i container osservati da CrowdStrike privi di protezioni di sicurezza correttamente configurate

36%
gli ambienti cloud che presentavano impostazioni predefinite del provider di servizi cloud non sicure

Identità del cloud come nuovo perimetro

Come nuovo perimetro, le identità sono assurte a chiavi del regno. I cybercriminali si concentrano meno sulla disattivazione delle tecnologie antivirus e firewall e più sulla modifica dei processi di autenticazione e sull'attacco alle identità. L'adozione continua di applicazioni e servizi basati sul cloud aumenta il numero di identità che un avversario può prendere di mira e utilizzare a proprio vantaggio.

Account utente legittimi sono stati sfruttati per ottenere l'accesso iniziale
nel **43%** delle intrusioni nel cloud

47% di configurazioni critiche errate nel cloud
legate all'integrità insufficiente di identità e diritti

Nel **67%** degli incidenti di sicurezza nel cloud, **CrowdStrike ha individuato ruoli di gestione dell'identità e degli accessi con privilegi più alti del necessario, a indicare che un avversario potrebbe aver manipolato il ruolo per compromettere l'ambiente e spostarsi lateralmente**

CrowdStrike per la sicurezza del cloud

La diffusione degli ambienti cloud procederà di pari passo con l'incremento dei relativi attacchi. È impossibile individuare tutte le vulnerabilità del cloud, le configurazioni errate e gli errori degli utenti, per non parlare della comprensione di tutte le tattiche, gli strumenti e le procedure in evoluzione utilizzate dai cybercriminali. Le organizzazioni non possono farcela da sole: hanno bisogno di un partner che conosca a fondo il comportamento dei cybercriminali e il cloud.

Come primo fornitore al mondo in ambito di rilevamento e risposta agli endpoint basati su agent, CrowdStrike ha adottato un approccio pionieristico alla progettazione di una sicurezza del cloud scalabile ed efficace che può essere implementata e gestita facilmente in un'unica piattaforma. CrowdStrike Falcon® Cloud Security è stato creato da zero per offrire una protezione sia agentless che agent-based. Le organizzazioni possono semplicemente attivarla ed estendere la protezione dai propri endpoint al cloud, coprendo l'intera infrastruttura IT con una protezione unificata e trasparente. Falcon Cloud Security riunisce la gestione della postura di sicurezza nel cloud, la protezione dei workload nel cloud e la gestione dei diritti di identità nel cloud in un'offerta completamente integrata di piattaforma di protezione delle applicazioni cloud native (CNAPP).

Scarica il white paper: Guida per gli addetti ai lavori alla difesa del cloud.

Ulteriori informazioni

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della sicurezza informatica, ha ridefinito la sicurezza moderna con la piattaforma native in cloud più avanzata al mondo per la protezione delle aree critiche del rischio aziendale: endpoint e workload cloud, identità e dati.

Con la tecnologia CrowdStrike Security Cloud e l'intelligenza artificiale di prima classe, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, le informazioni sulle minacce, lo spionaggio degli avversari in evoluzione e la telemetria arricchita provenienti da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'elite e osservabilità prioritaria delle vulnerabilità.

Costruita appositamente nel cloud con una singola architettura di lightweight-agent, la piattaforma Falcon assicura una distribuzione rapida e scalabile, protezione e prestazioni superiori, una complessità ridotta e un time-to-value immediato.

CrowdStrike: We stop breaches.

CROWDSTRIKE

Seguici

[1] https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023