Status sulle minacce informatiche: le tecniche di attacco alle reti cloud

Maggio 12, 2022
by Marco Rottigni, Technical Director Italia di SentinelOne

Lo scenario delle minacce alla sicurezza informatica continua ad ampliarsi e preoccupa ancora di più la combinazione delle tre "V": **Varianza, Volume, Velocità**. Tenersi aggiornati sulle tecniche e sulle nuove superfici di attacco è una sfida quotidiana, anche perché le aziende stanno migrando ai servizi in cloud che, inevitabilmente, sono oggetto costante di attenzione degli hacker. Nel testo, si riepilogano i più pericolosi metodi di attacco in cloud in circolazione e si dettaglia come i SentinelLabs li analizzano con attenzione.

1. Servizi vulnerabili

Una delle minacce più comunemente rilevate nelle reti cloud è la compromissione attraverso servizi vulnerabili, unitamente al fatto che una volta entrato nei sistemi l'hacker è potenzialmente in grado di fare qualunque azione. Ad esempio, attraverso i lateral movement, è consentito l'accesso ai sistemi e risorse aziendali ospitati in una rete cloud, e la sfida che le vittime devono vincere è quella di rispondere in modo efficace e tempestivo.

Un caso ben noto di questo tipo di attacco è stato lo sfruttamento immediato della vulnerabilità di Apache Log4J, che ha avuto un impatto critico in tutto il mondo. Le organizzazioni vittime che si sono affidate agli scanner di vulnerabilità per identificare e difendersi dai bugs come Log4j sono state esposte a un rischio maggiore nelle loro reti, poiché la vulnerabilità è stata sfruttata una settimana prima della sua divulgazione.

La gravità degli attacchi che si sono verificati sulla base di una vulnerabilità come Log4j dimostra quanto sia fondamentale per le aziende essere in grado di rilevare le attività dannose prima che un servizio sia noto come vulnerabile.

2. Configurazioni errate del cloud

La svista nelle configurazioni è la causa più comune delle principali fughe di dati nel cloud storage. Le organizzazioni che erroneamente lasciano i dati dei clienti pubblicamente o facilmente accessibili agli hacker hanno portato a un aumento costante della perdita dei dati nel corso degli anni. Anche in questo caso, non si tratta di un fenomeno esclusivo del cloud ma si conferma molto frequente, a causa della facilità e delle complessità richieste dalle configurazioni di storage nel cloud.

Inoltre, le errate configurazioni non si limitano a causare il furto dei dati. In molti casi i cloud hosting sono stati infettati da malware o da un ulteriore accesso alla rete a causa della capacità di un hacker di apportare modifiche al sistema. Ad esempio, il cyber criminale conosciuto come TeamTNT è capace di accedere a daemon Docker non protetti per installare ed eseguire le proprie azioni dannose, infettando le vittime con una botnet e cryptocurrency miners. Si tratta di una tecnica semplice ma molto efficace contro le organizzazioni con servizi cloud mal configurati.

3. Attacchi alla supply chain

Un metodo di attacco alla supply chain sempre più comune è la compromissione delle applicazioni di Docker Hub. Il già citato TeamTNT ha compromesso e continua a compromettere le applicazioni di Docker Hub, causando l'infezione di chiunque installi e aggiorni i file. Nel loro caso, gli obiettivi primari includono funzionalità botnet più generiche e l'uso di miners. Gli amministratori di Docker devono prestare attenzione quando accettano nuove applicazioni, analogamente all'implementazione di software esterno nella rete.

In termini di supply chain, ci troviamo sempre più spesso, nostro malgrado, nella condizione di incrementare le opportunità per gli hacker: Il software può essere compromesso in modo semplice ma efficace. Nella compromissione di Codecov, uno strumento comunemente utilizzato nel ciclo di vita dello sviluppo del software è stato modificato attraverso un aggiornamento per includere una singola riga di codice che è rimasta invisibile per mesi. Attacchi di questo tipo continueranno a essere sempre più comuni, in particolare attraverso il software open source utilizzato a livello globale.

4. Accesso alla piattaforma di gestione del cloud

Esempi come quelli sopra riportati possono essere di grande insegnamento: buona parte delle minacce al cloud è incentrata sul desiderio di accedere alla piattaforma di gestione del cloud, in particolare agli account cloud privilegiati. È fondamentale difendersi dalle minacce del cloud perché offrono all'aggressore l'opportunità di superare la barriera di accesso alle informazioni o al controllo di un servizio normalmente affidabile.

Un aggressore con accesso privilegiato alla piattaforma di gestione di un servizio cloud, sia esso AWS GCP o Azure, può farsi strada in molti punti difficili da identificare. Grazie all'uso di strumenti open source come Purple Panda, un aggressore con le mani su credenziali rubate può automatizzare l'escalation dei privilegi nel cloud e identificare opportunità di lateral movement.

I modi in cui gli aggressori cercano di ottenere tale accesso sono, ancora una volta, molto diversificati. Ad esempio, sappiamo che gli aggressori opportunisti scrutano i repository online di codice e applicazioni (Github, Docker Hub) alla ricerca di chiavi divulgate per errore. Questo ha permesso loro di dare il via ad attacchi alla supply chain e al furto generale di dati in grandi quantità. Inoltre, cyber criminali mirati altamente capaci e dotati di buone risorse, come APT29, si impegnano deliberatamente nella ricerca di tale accesso per missioni sponsorizzate dallo Stato. Nel complesso, si tratta di un livello di accesso altamente desiderabile per qualsiasi aggressore, quindi dovrebbe essere della massima importanza per i difensori tenerne traccia.

Conclusioni

Gli attacchi orientati al cloud sono da sempre di grande interesse sia per gli aggressori opportunistici che per quelli più selettivi. Sebbene le tecniche utilizzate negli attacchi siano ampie e diversificate, in genere si basano molto sul fatto che le reti cloud sono estese, complesse e onerose da gestire. Questo rende le soluzioni di sicurezza per agent e container fondamentali per la difesa di ogni organizzazione da tutte le piattaforme cloud.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Come anticipare gli hacker nel 2022: vademecum per la cybersecurity
- 6 stereotipi sulla cybersecurity che ogni consiglio direttivo dovrebbe approfondire
- Da SentinelOne alcuni suggerimenti per proteggere l'Active Directory
- Come difendersi da misconfiguration, vulnerabilità e minacce in cloud
- Difendere l'impresa nel 2022 dai rischi della Digital Supply Chain
- Come misurare l'efficacia dei controlli di sicurezza in 4 step