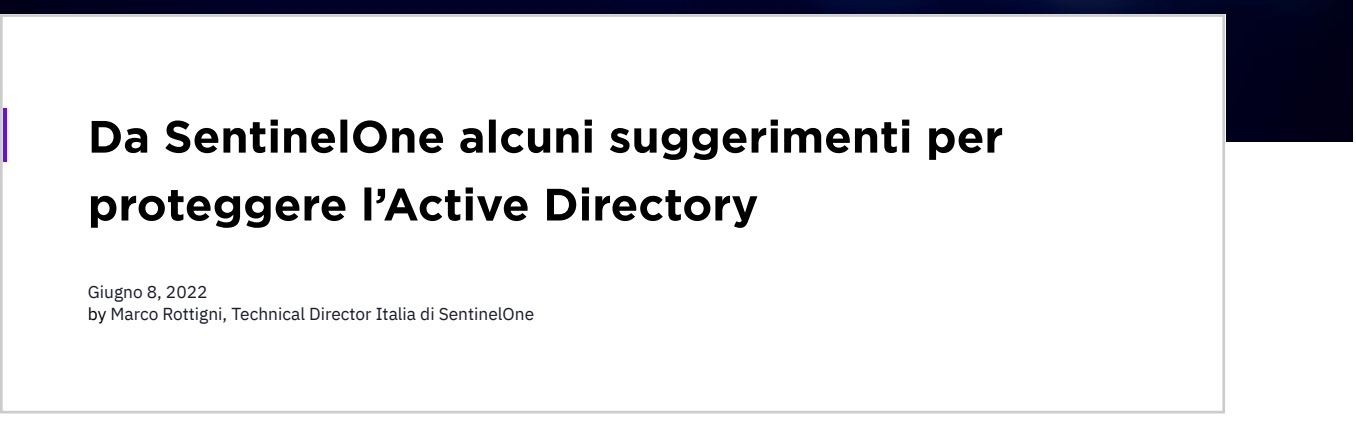
Da SentinelOne alcuni suggerimenti per proteggere l’Active Directory

Giugno 8, 2022
by Marco Rottigni, Technical Director Italia di SentinelOne

Active Directory (AD) è un obiettivo piuttosto ambito per gli hacker. Spesso, infatti, tentano di compromettere il sistema per incrementare i propri privilegi e poter accedere alla rete informatica. Sfortunatamente, i livelli funzionali dell’AD impongono che sia facilmente accessibile agli utenti di tutta l’azienda, il che rende l’ambiente operativo notoriamente difficile da proteggere. Microsoft ha evidenziato la gravità del problema dichiarando che più di 95 milioni di account AD vengono attaccati ogni giorno. Proteggere l’AD è una sfida, ma non è impossibile: richiede solo gli strumenti e le tattiche giuste. Di seguito alcune indicazioni per proteggere più efficacemente l’AD dalle più comuni tattiche di attacco.



1. Ridurre e monitorare il numero di sessioni privilegiate, di accessi diretti, di servizio e di rete

Una volta che un hacker ha violato le difese perimetrali e ha stabilito un punto d’appoggio all’interno della rete, effettuerà una rilevazione per identificare le risorse potenzialmente preziose e il percorso per raggiungerle. Uno dei modi migliori per farlo è prendere di mira l’AD, camuffando le proprie azioni come normali attività con poche possibilità di essere individuato.

La capacità di rilevare e controllare il numero dei privilegi, degli accessi diretti e degli account di servizio può allertare i responsabili di sicurezza sulla presenza di un hacker già nelle prime fasi del ciclo di attacco. Anche la distribuzione di account e credenziali di dominio ingannevoli sugli endpoint può mettere in difficoltà gli aggressori e consentire al team interno di re-indirizzarli verso esche fasulle.

2. Identificare e correggere le esposizioni degli account privilegiati

Gli utenti spesso memorizzano le credenziali sulle proprie postazioni di lavoro, accidentalmente o volontariamente. I cyber criminali lo sanno e prendono di mira le credenziali memorizzate per accedere all’ambiente di rete. Il giusto set di credenziali può essere molto importante e gli intrusi cercheranno sempre di aumentare i propri privilegi e le possibilità di accesso. Le aziende possono evitare di esporre agli hacker una via d’accesso facile alla rete identificando le esposizioni agli account privilegiati, rimediando alle configurazioni errate e rimuovendo le credenziali salvate, le cartelle condivise e altre vulnerabilità.

3. Proteggere e rilevare gli attacchi “Golden Ticket” e “Silver Ticket”

Gli attacchi Pass-the-Ticket (PTT) sono tra le tecniche più potenti utilizzate dagli hacker per muoversi lateralmente in rete e aumentare i privilegi. La strategia di progettazione stateless di Kerberos ne facilita l’abuso, il che significa che gli aggressori possono facilmente falsificare i ticket all’interno del sistema. Il “Golden Ticket” e il “Silver Ticket” sono due dei tipi di attacco PTT più gravi utilizzati per ottenere la compromissione del dominio. Per risolvere questo problema occorre poter rilevare gli account di servizio informatico e i Ticket Granting Ticket (TGT) Kerberos vulnerabili, identificando e segnalando le configurazioni errate che potrebbero potenzialmente portare ad attacchi PTT. Inoltre, una soluzione come Singularity Identity può impedire l’uso di ticket contraffatti negli endpoint.

4. Protezione contro gli attacchi Kerberoasting, DCSync e DCShadow

Un attacco “Kerberoasting” è un modo semplice per gli attaccanti di ottenere accesso privilegiato, mentre gli attacchi DCSync e DCShadow servono per mantenere persistenza nel dominio dell’azienda. I responsabili della sicurezza devono essere in grado di eseguire una valutazione continua dell’AD che fornisca un’analisi in tempo reale degli attacchi all’AD e avvisi sulle configurazioni errate che portano a tali attacchi. In aggiunta, una soluzione in grado di utilizzare misure di prevenzione a livello di endpoint, per impedire ai malintenzionati di scoprire gli account da colpire, può inibire la loro capacità di effettuare queste incursioni.

5. Prevenire l’acquisizione di credenziali dalle condivisioni di dominio

Gli hacker puntano comunemente alle password in chiaro o reversibili memorizzate negli script o nei file dei criteri di gruppo, archiviati nelle condivisioni di dominio come Sysvol o Netlogon. Una soluzione come Ranger AD può aiutare a rilevare queste password, consentendo ai responsabili interni di rimediare alle esposizioni prima che gli hacker possano prenderle di mira. Meccanismi come quelli di Singularity Identity possono anche distribuire nel sistema AD oggetti di criteri di gruppo Sysvol ingannevoli, che contribuiscono a deviare deviare l’attenzione dell’attaccante dalle risorse di produzione.

6. Identificare gli account con SID con privilegi nascosti

Utilizzando tecniche di *injection* dell’identificatore di sicurezza (SID) di Windows, gli avversari possono sfruttare l’attributo “history” del SID; ciò consente loro di spostarsi lateralmente all’interno dell’ambiente AD e di aumentare ulteriormente i propri privilegi. Per evitare che questo accada, è necessario rilevare gli account impostati con valori SID privilegiati noti nell’attributo SID della cronologia e nei rapporti.

7. Rilevare la delega dei diritti di accesso pericolosi sugli oggetti critici

La delega è una funzione di AD che consente a un utente o a un account di computer di sostituirsi a un altro account. Ad esempio, quando un utente chiama un’applicazione web ospitata su un server web, l’applicazione può imitare le credenziali dell’utente per accedere alle risorse ospitate su un server diverso. Qualsiasi computer di dominio con delega non vincolata abilitata può prendere le credenziali dell’utente a qualsiasi altro servizio del dominio. Purtroppo, gli attaccanti possono sfruttare questa funzione per accedere a diverse aree della rete. Il monitoraggio continuo delle vulnerabilità AD e delle esposizioni alla delega può aiutare i responsabili interni a identificare e correggere queste vulnerabilità prima che si possa sfruttarle per scopi malevoli.

8. Identificare gli account privilegiati con delega abilitata

A proposito di delega, gli account privilegiati configurati con delega non vincolata possono portare direttamente ad attacchi Kerberoasting e Silver Ticket. Le aziende devono essere in grado di rilevare e segnalare gli account privilegiati con delega abilitata. Un elenco completo di utenti privilegiati, amministratori diretti e account di servizio può aiutare i responsabili interni a fare il punto sulle potenziali vulnerabilità. In questo caso, la delega non è automaticamente negativa. Spesso è necessaria per un motivo operativo, ma i responsabili interni possono utilizzare uno strumento come Singularity Identity per impedire agli hacker di scoprire tali account.

9. Identificare gli utenti non privilegiati nell’ACL AdminSDHolder

I servizi di dominio di Active Directory (AD DS) utilizzano l’AdminSDHolder e il processo Security Descriptor Propagator (SDProp) per proteggere gli utenti e i gruppi privilegiati. L’AdminSDHolder ha un elenco di controllo degli accessi (ACL) unico, che verifica le autorizzazioni dei presidi di sicurezza che sono membri di gruppi AD privilegiati integrati. Per consentire il movimento laterale, gli attaccanti possono aggiungere account all’AdminSDHolder, concedendo loro lo stesso accesso privilegiato di altri account protetti. Le organizzazioni possono prevenire questa attività con uno strumento come Ranger AD per rilevare e segnalare la presenza di account insoliti all’interno dell’ACL AdminSDHolder.

10. Identificare le modifiche recenti ai criteri di dominio o controller predefiniti

All’interno di AD, le organizzazioni utilizzano i criteri di gruppo per gestire diverse configurazioni operative, definendo impostazioni di sicurezza specifiche per l’ambiente. Spesso configurano gruppi amministrativi e includono script di avvio e spegnimento. Gli amministratori li configurano per impostare i requisiti di sicurezza definiti dall’organizzazione a ogni livello, installare software e impostare le autorizzazioni dei file e del registro. Purtroppo, gli hacker possono modificare questi criteri per ottenere la persistenza del dominio all’interno della rete. Il monitoraggio delle modifiche ai criteri di gruppo predefiniti può aiutare i responsabili interni a individuare rapidamente questi aggressori, riducendo i rischi per la sicurezza e aiutando a prevenire l’accesso privilegiato all’AD.

Adottare gli strumenti giusti

Comprendere le tattiche più comuni utilizzate dagli avversari per colpire l’AD può aiutare le aziende a difendere il sistema. Nello sviluppo di strumenti come Ranger AD e Singularity Identity, SentinelOne ha preso in considerazione molti vettori di attacco e ha identificato il modo migliore per rilevarli e bloccarli. Grazie a questi strumenti, oggi le aziende possono identificare efficacemente le vulnerabilità, rilevare tempestivamente le attività dannose e porre rimedio agli incidenti di sicurezza prima che gli intrusi possano aumentare i loro privilegi e trasformare un attacco su piccola scala in una grave violazione. Proteggere l’AD è una sfida, ma non è irraggiungibile, grazie agli strumenti di protezione dell’AD oggi offerti.

Per ulteriori informazioni consultare it.sentinelone.com

Read more about Cyber Security

- Mettere in sicurezza le infrastrutture informatiche critiche delle nazioni
- Sicurezza di Active Directory | Che cos’è e cosa occorre sapere