BadSuccessor: vulnerabilità negli ambienti Active Directory Enterprise



Nel panorama della cybersecurity moderna, poche scoperte hanno avuto l'impatto della vulnerabilità BadSuccessor identificata dai ricercatori di Akamai nel maggio 2025. Questa falla di sicurezza rappresenta un perfetto esempio di come le innovazioni progettate per migliorare la sicurezza possano paradossalmente aprire nuovi vettori di attacco.

La storia inizia con le migliori intenzioni, Microsoft aveva introdotto in Windows Server 2025 una nuova funzionalità chiamata Delegated Managed Service Accounts (dMSA), pensata per risolvere uno dei problemi più persistenti nella gestione delle identità enterprise – gli attacchi di Kerberoasting. Tuttavia, come spesso accade nel mondo della sicurezza informatica, la soluzione ha creato un problema ancora più grave.

Yuval Gordon, ricercatore di sicurezza presso Akamai, ha scoperto che questa nuova funzionalità può essere sfruttata per compromettere qualsiasi utente in Active Directory, inclusi i Domain Administrator, utilizzando privilegi apparentemente innocui che molti utenti già possiedono.

La vulnerabilità BadSuccessor: anatomia di un attacco sofisticato

Cosa sono i Delegated Managed Service Accounts

Per comprendere la gravità di BadSuccessor, dobbiamo prima spiegare cosa sono i dMSA e perché Microsoft li ha introdotti. I Delegated Managed Service Accounts rappresentano

l’evoluzione degli account di servizio tradizionali utilizzati dalle applicazioni per autenticarsi nei domini Active Directory.

Storicamente, gli account di servizio hanno rappresentato un punto debole nella sicurezza enterprise. Questi account utilizzano password statiche che raramente vengono cambiate, rendendoli vulnerabili agli attacchi di Kerberoasting – una tecnica che permette agli attaccanti di estrarre e craccare offline le password degli account di servizio.

I dMSA dovevano risolvere questo problema attraverso:

1. **Rotazione automatica delle password**: Le credenziali vengono cambiate automaticamente senza intervento umano;
2. **Binding alle identità macchina**: L’autenticazione è legata a specifiche macchine, limitando l’uso improprio delle credenziali:
3. **Migrazione trasparente**: Gli account di servizio esistenti possono essere migrati verso dMSA senza interruzioni operative.

Come funziona l’attacco BadSuccessor

La vulnerabilità sfrutta il meccanismo di migrazione dei dMSA in modo estremamente sofisticato. Ecco come procede un attaccante:

Fase 1: Creazione del dMSA Malicioso
L’attaccante crea un nuovo dMSA utilizzando permessi CreateChild su qualsiasi Organizational Unit (OU) del dominio. Questi permessi sono comunemente assegnati per operazioni di amministrazione di routine e spesso non destano sospetti.

Fase 2: Manipolazione degli Attributi Critici
L’attacco si basa sulla modifica di due attributi specifici:

- msDS-ManagedAccountPrecededByLink: Viene impostato per puntare all’account target che si vuole compromettere

(ad esempio, un Domain Admin);
- msDS-DelegatedMSAState: Viene configurato per simulare una migrazione in corso

Fase 3: Impersonificazione Automatica
Il Key Distribution Center (KDC) di Active Directory, vedendo questi attributi, assume che il dMSA stia legittimamente sostituendo l'account target e gli concede automaticamente tutti i privilegi e le appartenenze ai gruppi dell'account originale.

L'aspetto più pericoloso: nessun permesso richiesto sull'account target

Quello che rende BadSuccessor particolarmente insidioso è che l'attaccante non ha bisogno di alcun permesso diretto sull'account che vuole compromettere. Come spiega Gordon: "*È sufficiente avere permessi di scrittura sugli attributi di un dMSA per compromettere qualsiasi utente del dominio.*"

Questo significa che un utente con privilegi apparentemente limitati può scalare i propri privilegi fino a diventare Domain Administrator senza lasciare tracce evidenti nelle configurazioni degli account target.

L'impatto reale: numeri che fanno riflettere

Una vulnerabilità sistemica, non un caso isolato

Le ricerche condotte da Akamai hanno rivelato la portata allarmante del problema. In 91% degli ambienti Active Directory esaminati, sono stati trovati utenti al di fuori del gruppo domain admins con i permessi necessari per eseguire questo attacco. Questo dato trasforma BadSuccessor da una curiosità teorica in una minaccia concreta per la stragrande maggioranza delle organizzazioni enterprise.

Esposizione universale

Un aspetto particolarmente preoccupante è che la vulnerabilità diventa disponibile in qualsiasi dominio che abbia almeno un domain controller Windows Server 2025, anche se l'organizzazione non utilizza attivamente i dMSA. Questo significa che le organizzazioni potrebbero essere vulnerabili semplicemente per aver aggiornato i loro domain controller, senza aver mai configurato o utilizzato la nuova funzionalità.

La controversia: Microsoft vs. Akamai sulla severità

Due visioni diverse del rischio

La scoperta di BadSuccessor ha generato un dibattito significativo sulla valutazione del rischio cybersecurity. Microsoft ha classificato la vulnerabilità come "moderata severità" e ha dichiarato che non soddisfa i criteri per una patch immediata, sostenendo che l'exploitation richiede permessi specifici sull'oggetto dMSA, indicativi di privilegi già elevati.

Tuttavia, i ricercatori di Akamai contestano fermamente questa valutazione, sottolineando che i modelli di delega diffusi nelle enterprise moderne rendono i diritti di creazione dMSA tutt'altro che rari.

Il problema dei "Shadow Admin"

Gordon spiega che nelle organizzazioni moderne, i permessi CreateChild vengono spesso assegnati per supportare modelli di delega operativa. Questi "shadow admin" – utenti con privilegi limitati ma specifici – possono non essere considerati a rischio elevato nelle valutazioni di sicurezza tradizionali, ma BadSuccessor dimostra come questi privilegi apparentemente benigni possano essere trasformati in chiavi per il regno digitale.

Strategie di mitigazione e *best practices*

Misure immediate di protezione

In assenza di una patch ufficiale, le organizzazioni devono implementare misure di mitigazione proattive:

Audit dei Permessi dMSA
Akamai ha rilasciato uno script PowerShell che enumera tutti i principali non predefiniti che possono creare dMSA e elenca le Organizational Unit in cui ciascun principale ha questo permesso. Questo strumento è essenziale per comprendere l'esposizione attuale.

Restrizione dei Privilegi
Le organizzazioni dovrebbero limitare immediatamente i permessi per creare dMSA esclusivamente ad amministratori fidati e documentati. Questa misura riduce significativamente la superficie di attacco.

Implementazione del Monitoraggio
È cruciale implementare logging e monitoraggio per:

- Eventi di creazione dMSA;
- Modifiche agli attributi msDS-ManagedAccountPrecededByLink e msDS-DelegatedMSAState;
- Eventi di autenticazione dMSA anomali.

Principi di sicurezza a lungo termine

BadSuccessor sottolinea l'importanza di applicare consistentemente il principio del privilegio minimo. Le organizzazioni devono rivedere sistematicamente le assegnazioni di permessi, specialmente quelli che sembrano innocui ma possono essere concatenati per escalation dei privilegi.

L’evoluzione del panorama cybersecurity nel 2025

NIST Cybersecurity Framework 2.0: una nuova era

La scoperta di BadSuccessor coincide con significativi sviluppi nelle linee guida di sicurezza nazionali. NIST ha aggiornato il Privacy Framework per mantenerlo allineato con il Cybersecurity Framework 2.0, rilasciato nel febbraio 2024. Questo aggiornamento enfatizza la governance come funzione elevata, sottolineando che la cybersecurity deve essere integrata nella strategia complessiva dell’organizzazione.

Executive Order 2025: mandati governativi per la sicurezza

L’Executive Order del gennaio 2025 “Strengthening and Promoting Innovation in the Nation’s Cybersecurity” ha incaricato NIST di migliorare l’accountability per i fornitori di software e servizi cloud. Questo mandato include lo sviluppo di aggiornamenti al Secure Software Development Framework (SSDF) e la promozione dell’uso innovativo di tecnologie emergenti nella cybersecurity.

L’importanza della ricerca proattiva

NIST deve ora dare priorità alla ricerca su metodi di interazione uomo-AI per l’analisi cyber difensiva e per rendere più sicura l’assistenza AI nella programmazione. Questa direzione riflette la crescente consapevolezza che il 40% di tutti gli attacchi cyber è ora guidato dall’AI.

Zero Trust: dal concetto alla realtà operativa

L’accelerazione dell’adozione Zero Trust

Il caso BadSuccessor illustra perfettamente perché le architetture Zero Trust stanno diventando essenziali. Gartner prevede che il 60% delle enterprise adotterà ‘Zero Trust’ come punto di partenza per la sicurezza nel 2025, riflettendo un cambiamento paradigmatico fondamentale.

I 3 pilastri dello Zero Trust

Il modello Zero Trust, come definito nel framework NIST 800-207, si basa su tre principi che sono direttamente applicabili alla mitigazione di vulnerabilità come BadSuccessor:

“Never Trust, Always Verify”
Questo principio richiede che nessuna entità – utente, dispositivo o applicazione – sia considerata fidata per default. Nel contesto di BadSuccessor, significa che ogni richiesta di creazione o modifica dMSA deve essere verificata e autorizzata esplicitamente.

Accesso condizionale basato sul rischio
L’accesso dovrebbe essere concesso basandosi su una valutazione dinamica del rischio. Le organizzazioni possono implementare controlli che richiedono approvazioni aggiuntive per operazioni sui dMSA basate su fattori di rischio contestuali.

Assunzione di violazione
Questo principio assume che le violazioni possano verificarsi in qualsiasi momento, richiedendo monitoraggio continuo e segmentazione per limitare l’impatto laterale.

L’integrazione dell’AI nelle architetture Zero Trust

L’intelligenza artificiale sta diventando centrale nelle architetture Zero Trust del 2025, con AI e machine learning che automatizzano il rilevamento delle minacce, il controllo

degli accessi e la detection delle anomalie. Questa evoluzione è particolarmente rilevante per identificare pattern di comportamento anomali che potrebbero indicare exploitation di vulnerabilità come BadSuccessor.

Impatti settoriali: il caso dell'healthcare

Una tempesta perfetta di vulnerabilità

Il settore sanitario offre un esempio illuminante dell'impatto potenziale di BadSuccessor. Le organizzazioni sanitarie hanno affrontato sfide cybersecurity senza precedenti nel 2025, con oltre 133 milioni di cartelle cliniche esposte nel 2024 e un costo medio delle violazioni che ha raggiunto $11 milioni.

Ransomware e downtime critico

Il ransomware rappresenta ora il 71% di tutti gli attacchi contro le organizzazioni sanitarie, causando un downtime medio di 11 giorni per incidente. In questo contesto, una vulnerabilità che permette la compromissione completa di Active Directory assume una criticità esistenziale.

Soluzioni innovative per la microsegmentazione

Le soluzioni Zero Trust nel settore sanitario stanno evolvendo verso approcci più sofisticati di microsegmentazione, con capacità di controllo dinamico delle policy basate su intelligence in tempo reale. Questi sviluppi sono direttamente applicabili alla mitigazione di vulnerabilità come BadSuccessor.

Tendenze nell'exploitation delle vulnerabilità: il quadro generale

Cambiamenti qualitativi nelle minacce

Mentre il numero totale di vulnerabilità note sfruttate (KEV) si è mantenuto relativamente stabile tra il quarto trimestre 2024 e il primo trimestre 2025, si osserva un cambiamento qualitativo significativo nei target degli attaccanti.

Focus sulle tecnologie enterprise

I sistemi di gestione dei contenuti (CMS) sono stati la categoria più popolare per i KEV nel primo trimestre 2025, con 35 flaw sfruttati, mentre Microsoft Windows (15) è stata la piattaforma più presa di mira. Questa tendenza sottolinea come le tecnologie enterprise stiano diventando obiettivi primari.

Prioritizzazione basata su metriche

NIST ha pubblicato il Cybersecurity White Paper 41, “Likely Exploited Vulnerabilities: A Proposed Metric for Vulnerability Exploitation Probability”, per aiutare le organizzazioni a identificare vulnerabilità attivamente sfruttate e misurare la prioritizzazione dopo il patching. Questo approccio quantitativo è essenziale per gestire efficacemente il volume crescente di vulnerabilità.

Password Policy e IAM: l’evoluzione delle best practices

Superare la complessità superficiale

Le linee guida NIST per le password raccomandano di eliminare le regole di composizione tradizionali (come l’obbligo di caratteri speciali) e di implementare controlli contro password precedentemente compromesse. Questa evoluzione riflette una comprensione più matura della sicurezza delle password.

Integration con Zero Trust

L’enfasi si è spostata dalla complessità all’efficacia, incoraggiando password più lunghe e uniche piuttosto che combinazioni prevedibili di caratteri speciali. Questo approccio è complementare ai principi Zero Trust, enfatizzando l’efficacia reale rispetto alla complessità apparente.

Raccomandazioni strategiche per le organizzazioni

Framework di gestione del rischio integrato

BadSuccessor dimostra la necessità di approcci olistici alla gestione del rischio cyber. Le organizzazioni moderne devono:

Implementare governance multi-livello
La cybersecurity deve essere integrata nelle decisioni architetturali fin dalle fasi iniziali di progettazione. Ogni nuova funzionalità deve essere valutata non solo per i benefici che apporta, ma anche per i nuovi vettori di attacco che potrebbe introdurre.

Adottare Zero Trust incrementalmente
L’implementazione di Zero Trust deve essere graduale, bilanciando sicurezza e operatività. Le organizzazioni possono iniziare con controlli granulari su funzionalità critiche come i dMSA, espandendo progressivamente l’approccio.

Sviluppare capacità di Threat Intelligence
L’investimento in intelligence proattiva è essenziale per identificare vettori di attacco emergenti prima che diventino mainstream.

Testing di Sicurezza Proattivo

La scoperta di BadSuccessor sottolinea l’importanza di:

- **Red Team Exercises**: Team di sicurezza interni o esterni

dovrebbero regolarmente testare nuove funzionalità per identificare potenziali abuse cases;
- **Threat Modeling**: Ogni nuova implementazione dovrebbe includere una valutazione sistematica dei possibili vettori di attacco;
- **Continuous Security Assessment**: I controlli di sicurezza devono essere rivalutati ogni volta che vengono introdotte nuove funzionalità.

Il futuro della cybersecurity: lezioni da BadSuccessor

L'Importanza della Collaborative Disclosure

Il caso BadSuccessor evidenzia la necessità di processi di disclosure migliorati che bilancino trasparenza e mitigazione del rischio. La decisione di Akamai di pubblicare i dettagli completi dopo che Microsoft ha classificato la vulnerabilità come moderata solleva importanti questioni su come l'industria dovrebbe gestire le divergenze nella valutazione del rischio.

Continuous Monitoring come necessità

La natura di BadSuccessor – che sfrutta funzionalità progettate per migliorare la sicurezza – dimostra che il monitoraggio continuo non è più opzionale ma essenziale. Le organizzazioni devono sviluppare capacità per:

- Rilevare configurazioni anomale in tempo reale;
- Identificare pattern di comportamento che potrebbero indicare exploitation;
- Correlare eventi apparentemente disconnessi per identificare attacchi sofisticati.

L'evoluzione verso Security by Design

BadSuccessor rappresenta un caso di studio perfetto per l'importanza del "security by design". Le funzionalità future

devono essere progettate con controlli di sicurezza integrati fin dall'inizio, non aggiunti successivamente come afterthought.

Trasformare le sfide in opportunità

La vulnerabilità BadSuccessor, pur rappresentando una seria minaccia per la sicurezza enterprise, offre anche importanti opportunità di apprendimento e miglioramento. La sua scoperta evidenzia come la cybersecurity moderna richieda un approccio olistico che integri governance strategica, implementazione tecnica granulare e monitoraggio continuo.

BadSuccessor dimostra che la sicurezza non può essere considerata un obiettivo raggiungibile una volta per tutte, ma deve essere vista come un processo evolutivo che richiede adattamento continuo.

Le organizzazioni devono sviluppare la capacità di vedere i propri sistemi dalla prospettiva degli attaccanti, identificando come funzionalità apparentemente innocue possano essere concatenate per creare vettori di compromissione.

La scoperta e la disclosure di BadSuccessor evidenziano l'importanza della collaborazione tra ricercatori di sicurezza, vendor e organizzazioni utenti per identificare e mitigare le minacce emergenti.

NIST rimane il framework di cybersecurity più valorizzato per il secondo anno consecutivo, fornendo una base solida per affrontare sfide come BadSuccessor. L'evoluzione verso architetture Zero Trust, supportata da framework NIST aggiornati e mandati governativi, crea le condizioni per una sicurezza più robusta e adattiva.

Le organizzazioni che riusciranno a trasformare la gestione del rischio cyber da funzione reattiva a vantaggio competitivo proattivo saranno quelle meglio posizionate per prosperare

nell’ecosistema digitale del futuro. BadSuccessor, paradossalmente, può servire da catalizzatore per questa trasformazione, spingendo le organizzazioni ad adottare approcci di sicurezza più maturi e sofisticati.

La lezione finale di BadSuccessor è che nell’era della trasformazione digitale, la sicurezza efficace richiede non solo tecnologie avanzate, ma anche una comprensione profonda delle interdipendenze sistemiche e un impegno continuo verso l’evoluzione delle best practices. Solo attraverso questo approccio integrato le organizzazioni potranno navigare con successo la complessità crescente del panorama delle minacce cyber.

Bibliografia e Fonti:

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/badsuccessor-vulnerabilita/