Cyber AI di Darktrace: credenziali e-mail compromesse

I responsabili aziendali considerano raramente quanto sia preziosa la casella di posta elettronica aziendale fino a quando non finisce nelle mani sbagliate. Una volta che riescono ad accedervi, i pirati informatici possono scegliere tra un'ampia gamma di opzioni di attacco e punti su cui far leva. La facilità con cui i pirati informatici possono ottenere l'accesso, attraverso campagne di phishing, attacchi di brute force o scambi nel Dark Web, dovrebbe essere motivo di allarme.

In molti casi, i pirati saccheggeranno la casella di posta per i preziosi dati in essa contenuti. Informazioni personali da chat private e dettagli sensibili relativi alla fatturazione possono essere sfruttati per frodi o ricatti, mentre vecchi thread possono contenere informazioni aziendali estremamente riservate. Elenchi di clienti, listini prezzi e perfino roadmap e dettagli IP possono essere spesso trovati con una semplice ricerca.

In altri casi, i criminali useranno l'account come punto di lancio per le fasi successive di un attacco. I pirati possono rimanere tranquillamente in disparte per ricavare informazioni estremamente importanti su dirigenti o partner, riesaminare documenti, leggere conversazioni e imparare come mimetizzarsi quando colpiscono fatalmente. Come nelle acquisizioni degli account della supply chain, la capacità di leggere un'e-mail thread in corso e passare alla fase successiva con una risposta plausibile è spesso il modo più efficace per completare con successo un attacco senza destare sospetti.

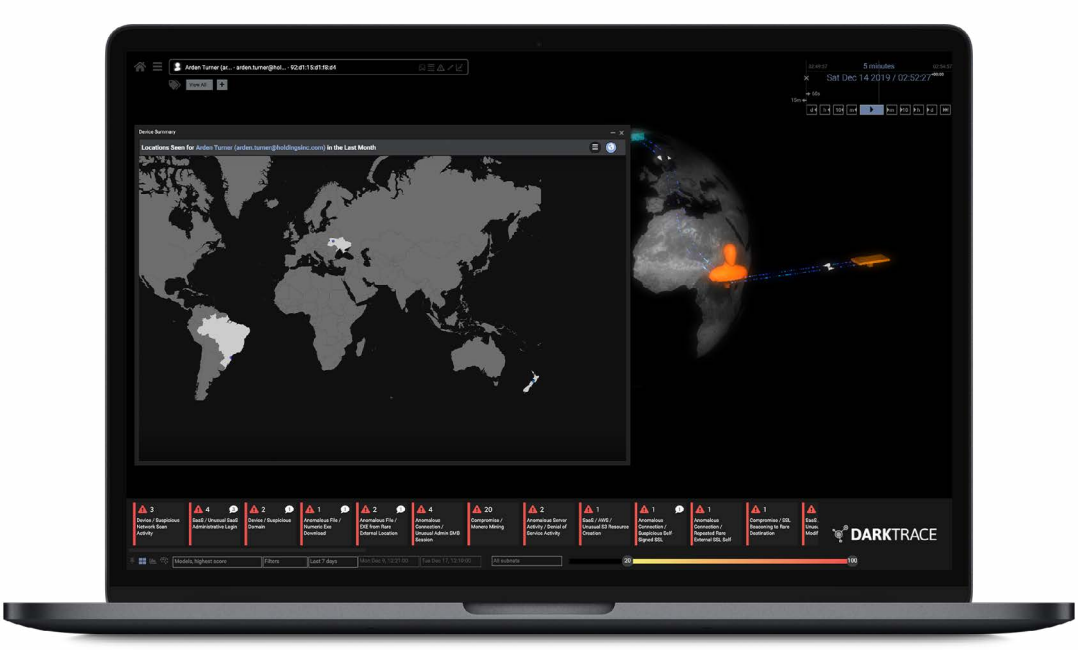

Figura 1: Threat Visualizer di Darktrace mostra le sedi geografiche di accesso.

Contesto aziendale completo

Se le possibilità dei pirati sono praticamente infinite, le opzioni per chi si difende sono limitate. Le acquisizioni di account aziendali sono tipicamente monitorate utilizzando difese semplici e statiche, incluse regole di "comunicazione impossibile" che raramente identificano i pirati informatici che sanno come nascondersi. Ma grazie alla sua visione estesa a tutta l'azienda, l'Enterprise Immune System di Darktrace completa questi approcci basati su regole individuando le minacce informatiche che inevitabilmente riescono ad eluderli.

Proprio come il sistema immunitario dell'uomo, la Cyber AI di Darktrace usa la conoscenza approfondita del "sé" per individuare comportamenti pericolosi che potrebbero altrimenti passare inosservati. Imparando il normale "pattern of life" di ogni utente e dispositivo che fa parte dell'azienda, Darktrace rileva le impercettibili deviazioni che identificano anche i pirati informatici più prudenti, deviazioni che si manifestano in comportamenti di accesso sospetti, creazione di regole per la posta in arrivo o modifiche ai permessi degli utenti. Poiché le minacce informatiche diventano più evolute, sfruttare l'AI di self-learning all'interno di tutto il business digitale sarà l'unica soluzione possibile per impedire che i pirati accedano alla casella di posta.

Case study 1: attacco di brute force automatizzato

Presso un'altra azienda, Darktrace ha rilevato numerosi tentativi di accesso non riuscito su un account Microsoft 365 eseguito tramite l'inserimento delle stesse credenziali, ogni giorno nel corso di una settimana. Ogni serie di tentativi di accesso era stata eseguita esattamente alle 18:04 per sei giorni. La coerenza sia dell'orario che del numero di tentativi di accesso relativi a ogni giorno era indicativa di un attacco di brute force automatizzato, programmato per interrompersi dopo un certo numero di tentativi non riusciti al fine di evitare blocchi.

Darktrace ha considerato questo pattern di tentativi falliti estremamente anomalo e, perciò, ha avvisato il team della sicurezza. Se Darktrace non avesse correlato questi deboli indicatori multipli e non avesse elaborato i segnali sottili di una minaccia emergente, questo attacco automatizzato avrebbe potuto continuare per settimane o mesi, facendo congetture studiate sulla password dell'utente sulla base di altre informazioni che aveva già acquisito.

Figura 2: Grafico che mostra i tentativi di accesso ripetuti

Case Study 2: compromissione e sabotaggio di un account Microsoft 365

In un'organizzazione no-profit internazionale, Darktrace ha rilevato il furto di un account Microsoft 365 che aveva bypassato la regola statica AD "comunicazione impossibile" di Azure. Anche se l'organizzazione ha uffici in ogni angolo del mondo, l' AI di Darktrace ha identificato un accesso da un indirizzo IP storicamente insolito per quell'utente e il suo gruppo di colleghi e ha immediatamente avvisato il team della sicurezza.

Darktrace ha poi segnalato che nell'account era stata impostata una nuova regola di elaborazione delle e-mail, che eliminava le e-mail in ingresso e quelle in uscita. Ciò indicava un chiaro segnale di compromissione e il team della sicurezza ha potuto bloccare l'account prima che il pirata informatico potesse fare danni.

Con l'attuazione di questa nuova regola per le e-mail, il pirata informatico avrebbe potuto avviare numerosi scambi con altri dipendenti dell'azienda, senza che l'utente legittimo lo scoprisse. Si tratta di una strategia comune usata dai pirati informatici che tentano di ottenere un accesso continuo e sfruttare numerosi punti di appoggio all'interno dell'organizzazione, potenzialmente in preparazione di un attacco su larga scala.

Analizzando il raro indirizzo IP e correlandolo con il comportamento anomalo del presunto utente, Darktrace ha identificato con certezza che si trattava di un caso di acquisizione di account, evitando problemi gravi all'azienda.