Attacco spoofing

Darktrace ha rilevato un attacco che aveva preso di mira un istituto finanziario di Atlanta, creato meticolosamente per indurre a fare clic su un link dannoso.

Il pirata informatico aveva registrato un dominio simile a quello dell'azienda presa di mira, ma che non vi corrispondeva esattamente. Ciò è possibile apportando piccole alterazioni al nome dell'azienda ma conservando l'aspetto del dominio originale: ad esempio una singola lettera nel nome o aggiungendo un trattino nel dominio.

Il pirata informatico era riuscito a inserirsi all'interno del flusso di scambio di e-mail. Una volta instaurata una serie di corrispondenze in ingresso e uscita, il pirata informatico ha sfruttato la fiducia creata per inviare un'e-mail contenente un link pericoloso.

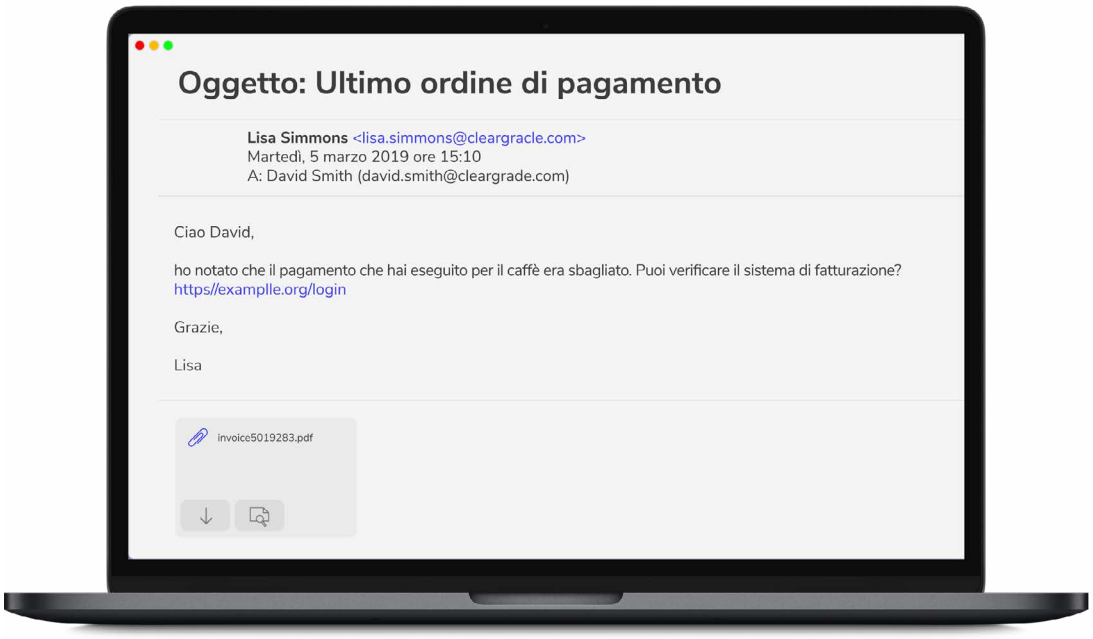

Figura 1: Un'e-mail in arrivo contenente un dominio falsificato.

Nell'immagine precedente dell'e-mail falsificata notare l'ortografia della parola "example". È una modifica impercettibile che il destinatario non ha notato e quindi ha fatto clic sul link. Ciò ha indirizzato l'utente ad un sito web ben realizzato che riproduceva perfettamente la pagine di accesso di Example.org, inducendo l'utente ad inserire le proprie credenziali, che vennerro acquisite dal pirata informatico, in grado ora di utilizzare le credenziali delle vittime in sistemi di pagamento legittimi.

Blocco dell'attacco con link di spoofing

Diversamente da qualsiasi altra soluzione, Antigena Email e l'Enterprise Immune System sono in grado di correlare il traffico in rete, nel Cloud e i dati delle e-mail per identificare se i domini associati a link e mittenti sono anomali, se la sede di un link contenuto in un'e-mail è insolita, se gli argomenti della discussione e i contenuti sono inusuali e anche se i pattern nel percorso URL sono sospetti.

Questo approccio fondamentale, unico nel suo genere, fa sì che il processo decisionale di Darktrace sia estremamente più preciso di quello di qualsiasi altro strumento, e per questo è in grado di intraprendere azioni altamente proporzionate e mirate per neutralizzare attacchi di phishing su vasta scala.

Darktrace non ha solo identificato il tentativo di impersonificazione, riconoscendo la somiglianza del nome nel dominio, ma ha anche rilevato che le e-mail avevano violato il modello "No Association", indicando che all'interno della sua intera conoscenza dell'ambiente delle e-mail e della rete dell'azienda, non aveva individuato alcun segno di relazione tra questo mittente e l'organizzazione.

Antigena Email ha risposto autonomamente per neutralizzare la minaccia bloccando l'accesso al link. Inoltre, è stato aggiunto un banner di allarme per informare gli utenti del team della sicurezza in merito alla potenziale minaccia. L'Enterprise Immune System di Darktrace era pronto ad intraprendere ulteriori azioni nel caso in cui il link fosse stato inviato ad altri utenti all'interno dell'azienda, impedendo così all'attacco di diffondersi ulteriormente.

Inoltre, la percentuale di esposizione degli utenti impersonificati era elevato, indicando che si trattava di obiettivi ad alto profilo, ovvero una violazione del modello "Whale Spoof". Comprendere che utenti interni chiave erano stati presi di mira ha consentito all'AI di Darktrace di dare priorità a questo attacco, avviando una risposta proporzionata in tempo reale.

Antigena Email: social engineering e adescamento

Gli attacchi di social engineering e adescamento riguardano tipicamente sofisticati tentativi di impersonificazione, in cui i pirati nascosti dietro false identità chiedono urgentemente ad un destinatario di rispondere, ricevere comunicazioni offline o eseguire transazioni offline. I loro obiettivi vanno dalla truffa bancaria allo spionaggio aziendale, fino al furtodi IP.Anche se le organizzazioni devono ovviamente investire in formazione sulla sicurezza ed istruire i propri dipendenti a riconoscere i segnali di allarme, nessuna mole di istruzioni è in grado di garantire un'immunità completa da questi attacchi sempre più sofisticati.

Mentre le tradizionali campagne di phishing generalmente includono payload dannosi nascosti dietro un link o un allegato, i tentativi di social engineering spesso coinvolgono l'invio di "e-mail sicure" che contengono solo testo. Questi attacchi superano facilmente gli strumenti di sicurezza esistenti, che fanno affidamento sulla correlazione tra link ed allegati e blacklist e firme. Inoltre, questo vettore di attacco generalmente coinvolge domini "sosia" di nuova registrazione, che non solo ingannano il destinatario, ma aggirano anche le difese tradizionali.

Antigena Email ha una conoscenza unificata di cosa è "normale" all'interno del traffico di e-mail e della rete che si evolve insieme all'azienda, consentendogli di rilevare anche i casi più nascosti di adescamento. Le e-mail pulite che superano le difese tradizionali possono essere identificate in pochi secondi grazie a una vasta gamma di metriche, incluse somiglianze sospette con utenti noti, associazioni anomale tra i destinatari interni e persino anomalie nel contenuto e nell'oggetto delle e-mail.

Il più delle volte, gli attacchi di social engineering mirano a mettere immediatamente offline la conversazione, il che significa che le misure di sicurezza lente e reattive tenderanno ad intervenire solo dopo che il danno è stato fatto. La sua efficace comprensione di ogni utente, dispositivo e relazione all'interno dell'organizzazione consente ad Antigena Email di rispondere proattivamente e con grande fiducia già la prima volta, intervenendo in questa importante fase iniziale.

Antigena Email è in grado di rispondere in numerosi modi, inclusi ma non limitati a: segnalazione al team della sicurezza, invio di un avviso ai destinatari delle e-mail allegando un banner di allarme al contenuto dell'e-mail, modifica o blocco dei link e blocco completo delle e-mail. Antigena vanta la capacità unica di adattare in maniera intelligente e autonoma le risposte a minacce specifiche.

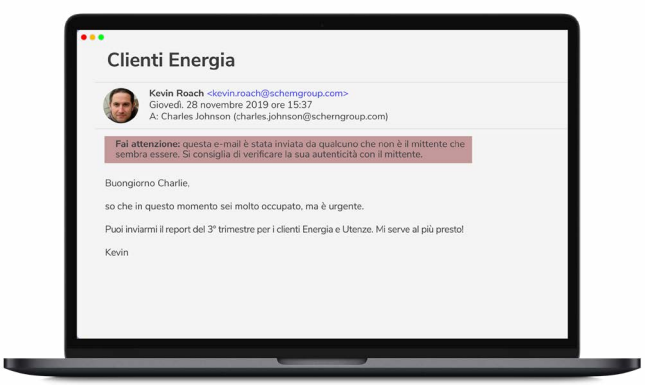

Figura 2: Un banner di allarme allegato ad un'email in arrivo falsificata con la richiesta di documenti aziendali sensibili.

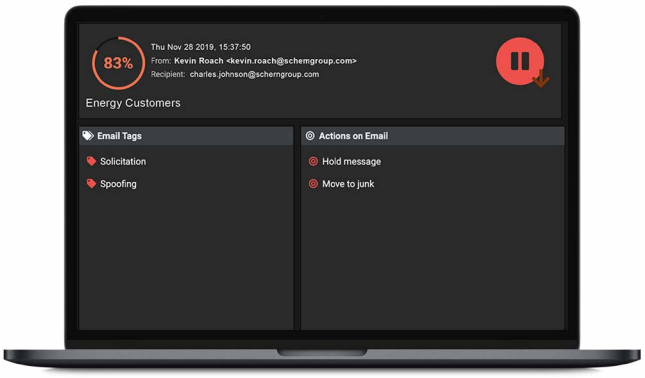

Figura 3: Antigena Email ha classificato l'e-mail precedente con l'83% di anomalia a causa dei segnali di adescamento e spoofing.

Contesto aziendale completo

Antigena Email di Darktrace è in grado di analizzare link e allegati nascosti correlati all'intero traffico di e-mail, nonché il "pattern of life" convenzionale dell'ambiente digitale. In caso di attacchi di phishing, Darktrace riconoscerà che né il destinatario né alcun altro nel gruppo di colleghi ha visitato in precedenza il dominio sospetto, generando un allarme di alta sicurezza e avviando in modo autonomo una risposta mirata.

Analizza anche la posizione del payload potenzialmente perioloso all'interno di un'e-mail, individuando ad esempio se è nascosto dietro vari pulsanti progettati per sembrare siti affidabili. Inoltre, analizza i pattern all'interno dell'indirizzo URL, confrontandolo con attacchi precedentemente bloccati al fine di individuare link sospetti. L'applicazione di questa ricchezza di contesto ad ogni e-mail in ingresso o in uscita all'interno dell'organizzazione consente ad Antigena Email di prendere autonomamente decisioni razionali, avviando una risposta mirata in tempo reale.

In base alla percezione della natura della minaccia, le azioni possibili includono il flattening degli allegati, il blocco di link pericolosi appena entrano nella rete e anche l'eliminazione retrospettiva delle e-mail dalla casella di posta in arrivo alla luce di nuove informazioni.