Antigena Email: social engineering e adescamento

Gli attacchi di social engineering sono caratterizzati in tutti i casi da un tentativo di sfruttare il persuasivo presupposto di fiducia all'interno di un'azienda. Fingendosi un collega, contatto o dirigente conosciuto e affidabile, i pirati informatici sono in grado di personalizzare le proprie comunicazioni di conseguenza e trovare rapidamente un punto di accesso all'interno dell'organizzazione, per richiedere il trasferimento fraudolento di denaro o convincere un dipendente a condividere documenti e informazioni aziendali sensibili. Questi attacchi avvengono tipicamente sotto forma di e-mail "pulite", che non contengono link o payload pericolosi, cosa che le rende quindi difficili da rilevare.

Poiché i pirati informatici continuano a sviluppare le proprie tattiche e tecniche, gli attacchi di social engineering e adescamento stanno diventando sempre più efficaci. Oggi è disponibile il software di machine learning in grado di apprendere lo stile con cui due utenti interagiscono e di replicare questi pattern di comunicazione. Ciò può essere sfruttato dai pirati informatici per impersonare in maniera convincente un contatto fidato, fino al punto che l'attività di differenziazione tra un'e-mail legittima e un attacco di social engineering guidato da AI diventa quasi impossibile.

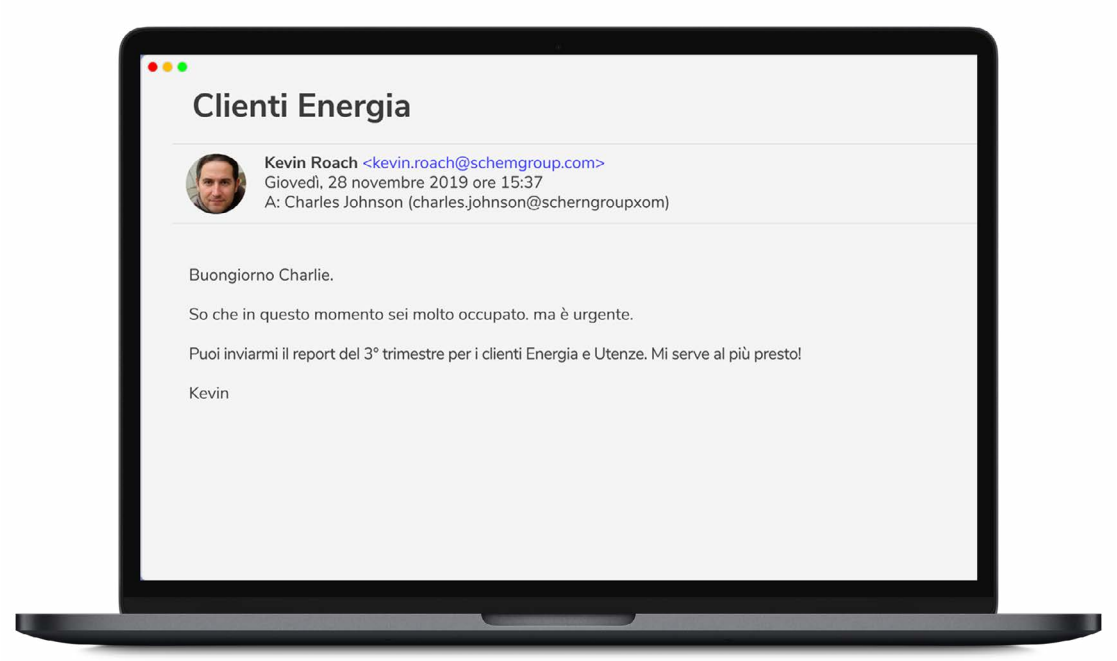

Figura 1: Un pirata si finge un dirigente, tentando di sfruttare documenti sensibili. Notare l'indirizzo e-mail falsificato.

Antigena Email: un approccio di tipo "Immune System"

Fornendo un approccio fondamentalmente unico in quest'area, Antigena Email utilizza l'AI di self-learning per aiutare le organizzazioni a riconquistare il vantaggio. La tecnologia sfrutta la Cyber AI per analizzare tutto il traffico e-mail in ingresso, uscita e laterale, consentendogli di apprendere le dinamiche umane e relazionali che sono alla base delle e-mail. Questa conoscenza approfondita consente ad Antigena di rilevare immediatamente le minacce, cosa fondamentale nel caso di attacchi di adescamento, il cui obiettivo spesso è spostare la conversazione offline e bypassare le misure di sicurezza.

Diversamente dalle difese tradizionali iniziali, che fanno affidamento su informazioni retrospettive, la comprensione personalizzata e in continua evoluzione che Darktrace ha di ciò che è "normale" consente ad Antigena Email di rispondere autonomamente agli attacchi di impersonificazione più impercettibili che hanno l'intenzione di eludere i gateway di posta elettronica. Il processo decisionale di Antigena Email è applicato anche durante tutto il ciclo di vita di un'e-mail, consentendo così al sistema di aggiornare le proprie analisi alla luce di nuove evidenze anche dopo che un'e-mail è stata recapitata. Grazie alla capacità di Antigena di monitorare continuamente anche dopo il recapito, il sistema è in grado di recuperare in maniera retroattiva le e-mail inviate, nel caso si rivelassero poi pericolose.

Case study: Antigena Email ha identificato preventivamente un'impersonificazione di livello C

Di recente Darktrace ha rilevato un tentativo di attacco di social engineering altamente mirato con il tentativo di impersonificare dirigenti di livello C presso un'azienda tecnologica statunitense. A quanto pare il pirata informatico aveva inviato numerose e-mail "pulite" nel tentativo di guadagnarsi la fiducia e stabilire comunicazioni offline, preludio di una richiesta di pagamento.

Era stata chiaramente eseguita una ricerca approfondita, poiché per ogni utente preso di mira il pirata informatico conosceva chi fosse il relativo dirigente di livello C, imitando questa persona nel suo tentativo di impersonificazione. Antigena Email ha identificato i tentativi di social engineering e come risultato ha bloccato tutte le e-mail dai destinatari previsti, seguendo questo processo:

1. Riconoscimento di oggetto e mittente anomali. L'e-mail conteneva il nome del dipendente preso di mira nell'oggetto e inoltre proveniva da un indirizzo Gmail apparentemente non correlato. Nonostante la mancanza di payload dannosi (come link o allegati), Antigena Email ha comunque identificato le e-mail come malevole.

2. Rilevazione di nessuna associazione. Antigena ha identificato i tentativi di impersonificazione non solo riconoscendo la somiglianza del nome nel dominio, ma anche che le e-mail avevano violato il modello "No Association". Ciò indicava che all'interno della sua intera conoscenza dell'ambiente di posta elettronica dell'azienda, Antigena non aveva individuato alcuna evidenza di relazione tra questo mittente e l'organizzazione.

3. Prevenzione di comunicazioni offline. Correlando questi numerosi indicatori di debolezza, Antigena ha riconosciuto queste e-mail come componenti di un unico attacco sistematico e le ha tenute in un buffer da sottoporre al controllo del team della sicurezza dell'organizzazione. Antigena ha riconosciuto che in questo caso si trattava dell'azione più appropriata, evitando che i destinatari presi di mira leggessero i contenuti delle e-mail e stabilissero comunicazioni offline.

4. Identificazione di spoofing. Antigena Email non ha solo identificato i tre dirigenti di livello C che erano stati impersonificati, ma ha anche riconosciuto che il pirata informatico stava utilizzando uno spoof dell'indirizzo personale esterno legittimo del CEO.

5. Rivelazione del whale spoof. Inoltre, la percentuale di esposizione degli utenti impersonificati era elevata, indicando che si trattava di obiettivi ad alto profilo soggetti ad un attacco di "Whale Spoof". Mentre le difese tradizionali installate non sono state in grado di rilevare l'attacco a causa della loro analisi statica e dell'ambito limitato, Antigena Email ha sfruttato la completa conoscenza degli utenti digitali dell'organizzazione e i loro "pattern of life" nella casella di posta in arrivo per neutralizzare la minaccia.

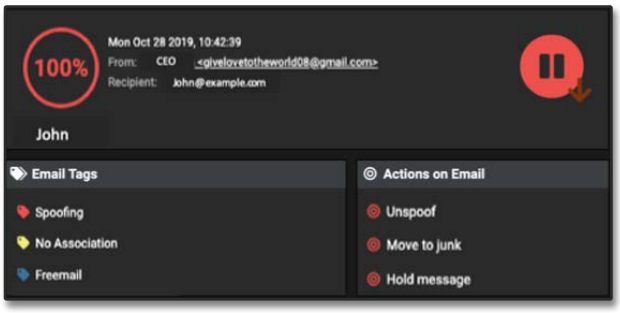

Figura 2: Una delle 30 e-mail, con una percentuale di anomalia del 100%

Figura 3: I modelli che hanno scatenato la risposta di Antigena Email

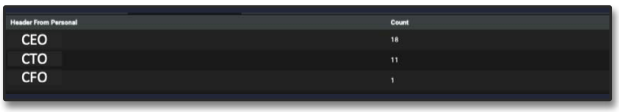

Figura 4: I tre dirigenti di livello C identificati

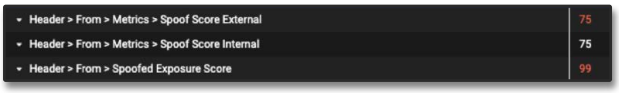

Figura 5: Antigena Email identifica il tentativo di spoofing