Antigena Email: acquisizione dell'account della Supply Chain

Rubando i dettagli dell'account di un contatto di fiducia nella supply chain, i pirati informatici sono in grado di guadagnarsi la fiducia di un destinatario e convincerlo a fare clic su un link pericoloso o anche a trasferire grandi somme di denaro fuori dall'azienda. Le difese delle e-mail esistenti presuppongono un rapporto di fiducia e questo significa che sofisticate acquisizioni di account passino spesso completamente inosservate.

I pirati informatici stanno utilizzando sempre più a proprio vantaggio le supply chain, compresi fornitori, partner e appaltatori, per infiltrarsi nelle organizzazioni. Nei primi mesi di quest'anno, un rapporto relativo al cosiddetto "island hopping", in cui i pirati informatici provano ad espandere una violazione all'interno di una supply chain, ha evidenziato che questo metodo è responsabile della metà degli attacchi di oggi.

I pirati che hanno accesso totale all'account e-mail di un fornitore sono in grado di studiare precedenti interazioni e-mail e produrre una risposta mirata all'ultima comunicazione. Il linguaggio che utilizzano appare spesso lecito, quindi gli strumenti di sicurezza e-mail esistenti che cercano parole o frasi chiave indicative di spoofing non saranno in grado di rilevare questi attacchi.

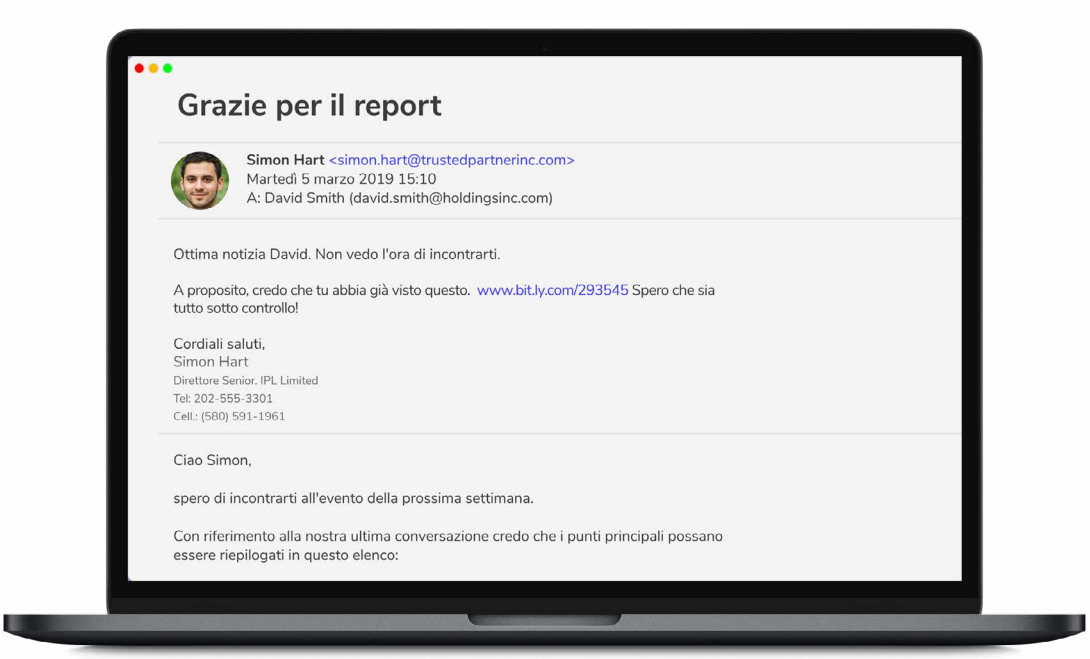

Figura 1: Una risposta plausibile inviata dall'account compromesso di un fornitore di fiducia. Il link conteneva un payload dannoso.

Antigena Email: distinguere gli amici dai nemici

Analizzando i pattern di comunicazione all'interno del traffico e-mail in ingresso, in uscita e laterale, Antigena Email di Darktrace utilizza un'ampia gamma di metriche per identificare con sicurezza casi di acquisizione di account, qualcosa che è impossibile rilevare senza una conoscenza dettagliata di ciò che è "normale" per ogni soggetto umano e e delle relazioni alla base degli indirizzi e-mail.

Antigena è in grado di analizzare più di 1.000 metriche per ogni e-mail, inclusi argomenti e contenuti, coerenza delle sedi di accesso e dei destinatari associati, insieme alla conoscenza del "pattern of life" del mittente. Antigena Email utilizza questa conoscenza di ciò che è "normale" per l'azienda, per stimare la probabilità che i contatti delle supply chain siano di fatto legittimi.

Quando identifica un'anomalia, Antigena interviene utilizzando l'Autonomous Response che, in base alla gravità della minaccia può variare la sua risposta dal bloccare link e allegati sospetti all'eliminare completamente un'e-mail dalla casella di posta in arrivo di un dipendente. Antigena Email si aggiorna continuamente alla luce di nuove evidenze, apprendendo in corso d'opera per garantire che la piattaforma di posta elettronica sia sempre protetta.

Case Study: Antigena Email ha identificato il furto dell'account di un fornitore

Un cliente che stava testando Antigena Email ha rilevato un grave incidente di sicurezza in cui l'account di un fornitore di fiducia è diventato la fonte di una campagna e-mail pericolosa. La tecnologia ha riconosciuto che il mittente era perfettamente noto all'azienda e numerosi utenti interni erano già entrati direttamente in contatto con lui in precedenza. Infatti, prima di quel giorno uno di questi utenti era coinvolto in una normale corrispondenza con l'account del fornitore che di lì a poco sarebbe stato rubato.

Meno di due ore dopo questo legittimo scambio di routine, il fornitore aveva inviato e-mail a 39 utenti, ognuna delle quali conteneva un link pericoloso. C'era una variazione nella riga dell'oggetto e nei link contenuti nelle e-mail e ciò suggeriva che si trattasse di e-mail altamente mirate da parte di un pirata informatico ben preparato. Lo scopo di questi link potrebbe essere stato quello di sollecitare pagamenti, raccogliere password o distribuire malware. Antigena Email ha identificato la gamma completa di segnali tipicamente associati all'acquisizione di account della supply chain, consigliando di bloccare tutte e 39 le e-mail in base a:

1. Sede di accesso insolita: Antigena Email ha determinato che le e-mail sono state inviate da un web server Outlook autentico. Questo elemento non era insolito per il fornitore, ma all'interno di questi dati di connessione è stato possibile anche estrarre l'indirizzo IP geo-localizzabile. Ciò indicava che il pirata informatico ha avviato il suo accesso da un IP negli Stati Uniti, a differenza della sede di accesso consueta nel Regno Unito.

2. Incongruenza dei link: i link pericolosi contenuti nelle e-mail erano tutti ospitati sulla piattaforma di sviluppo Microsoft Azure, probabilmente per aggirare le verifiche di reputazione sul dominio host. Nonostante la legittimità ampiamente riconosciuta di azurewebsites. net nel web, Antigena Email è stato in grado di rilevare che questo dominio era estremamente incoerente per il mittente, sulla base della cronologia della corrispondenza passata.

3. Destinatari insoliti: Una percentuale di "anomalia di associazione" viene assegnata per stimare la probabilità che questo particolare gruppo di destinatari possa ricevere un'e-mail dalla stessa fonte. Aggiungendo il contesto alla propria indagine nel corso del tempo, Antigena Email ha dedotto che questo gruppo di destinatari era anomalo al 100% già fin dalla terza e-mail.

4. Anomalia nell'argomento: le righe dell'oggetto di queste e-mail suggeriscono un tentativo di comunicare con un profilo basso e professionale. Pertanto, qualsiasi tentativo basato su firma per provare a cercare parole chiave associate al phishing fallirebbe. Tuttavia, Antigena Email ha riconosciuto che questi destinatari tipicamente non ricevevano e-mail relative a proposte commerciali che usavano questo genere di frasi.

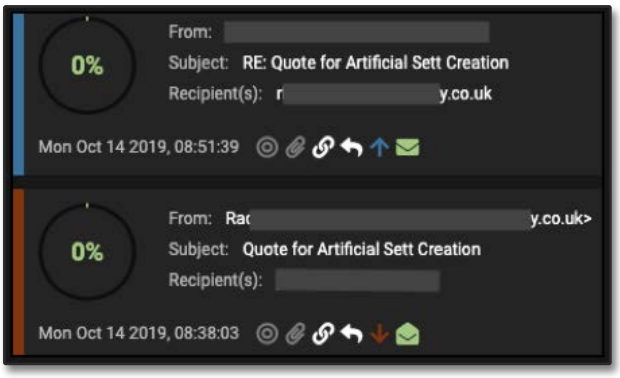

Figura 2: Precedente corrispondenza "normale" con il mittente, con una percentuale di anomalia pari allo 0%

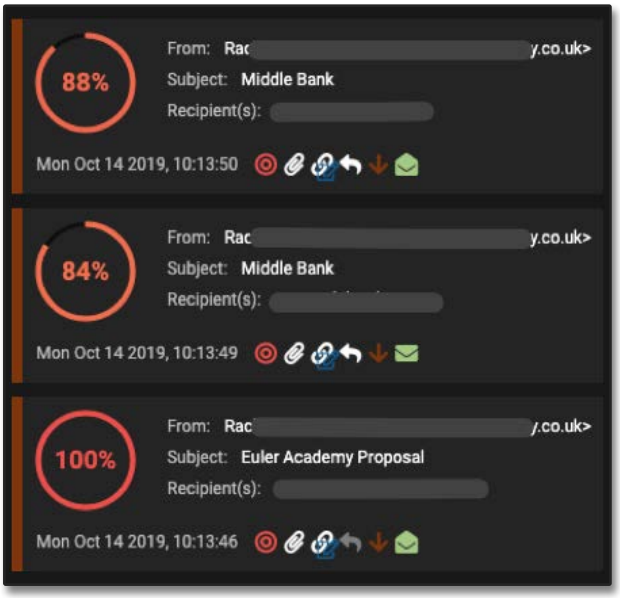

Figura 3: E-mail inviate più tardi lo stesso giorno contenenti allegati dannosi

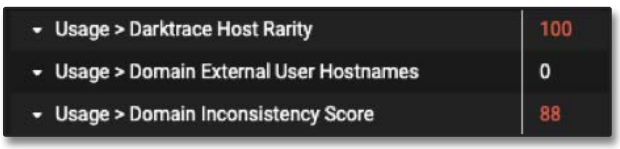

Figura 4: Modelli attivati da rarità e incoerenza del link

Figura 5: Antigena Email ha rilevato rapidamente che questo gruppo di destinatari non era strettamente correlato