Antigena Email: Spear phishing e payload

Di solito gli attacchi di phishing tentano di ingannare gli utenti inducendoli a fare clic su link o allegati dannosi contenuti in un'email, con l'obiettivo finale di acquisire credenziali o distribuire malware all'interno di un'organizzazione. Le e-mail possono essere lanciate come campagne indiscriminate "incrociate" contro migliaia di organizzazioni o come attacchi "spear phishing" creati appositamente e personalizzati per il destinatario.

La maggior parte degli strumenti di sicurezza per le e-mail fa affidamento sulla conoscenza di minacce identificate in precedenza, confrontando le e-mail in arrivo con blacklist predefinite al fine di determinare se sono pericolose o no. Queste soluzioni sono limitate al perimetro e analizzano solo le e-mail in isolamento. Inoltre, payload che contengono nuove specie di malware bypassano facilmente questo approccio obsoleto, lasciando l'azienda vulnerabile a questi attacchi evoluti.

Poiché gli attacchi che hanno origine dalle e-mail hanno iniziato ad utilizzare l'intelligenza artificiale, le e-mail di phishing sono sempre più raffinate e personalizzate per il destinatario, con payload dannosi spesso celati dietro link plausibili e pulsanti nascosti.

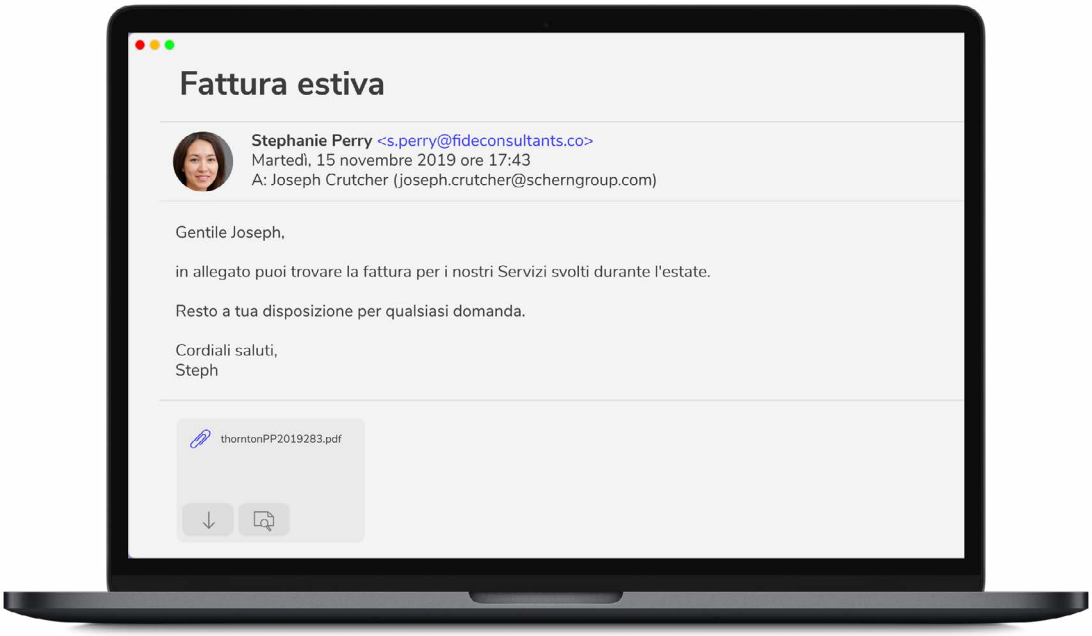

Figura 1: Un'e-mail che convince un dipendente a fare clic su un allegato che contiene un payload dannoso

Antigena Email: imparare i "Pattern of Life"

Antigena Email di Darktrace è in grado di analizzare link e allegati nascosti correlati alle comunicazioni in ingresso, uscita e a quelle laterali e con il contesto completo di quale sia il normale "pattern of life" per le dinamiche umane all'interno di ogni e-mail. In caso di attacchi di phishing, Antigena 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. Analizza anche la posizione del payload potenzialmente pericoloso all'interno di un'e-mail, individuando ad esempio se è nascosto dietro vari pulsanti progettati per sembrare siti affidabili.

Imparando il DNA digitale della piattaforma di posta elettronica di un'azienda, Antigena Email è in grado 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 flatt ning 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.

Case Study: Antigena Email ha bloccato un attacco di phishing via “WeTransfer”

Dopo solo una settimana dalla sua installazione, Antigena Email ha rilevato un sofisticato attacco e-mail che aveva preso di mira cinque utenti ad alto profilo. Le e-mail erano ben scritte e altamente plausibili e tentavano di convincere i destinatari a fare clic su un link pericoloso. Questo attacco avrebbe avuto facilmente successo se Antigena non avesse analizzato ogni e-mail in arrivo confrontandola con il “pattern of life” dell’organizzazione.

Le e-mail, apparentemente in arrivo da WeTransfer, avevano ricevuto una percentuale di anomalia del 100% e Antigena Email aveva suggerito di bloccarle e non recapitarle all’utente finale. Darktrace ha riconosciuto un link pericoloso nascosto e ha identificato anche i segnali di spoofing, nonostante l’organizzazione avesse un rapporto noto con il mittente.

Dai dati di connessione, si può vedere che non c’erano segnali evidenti nell’intestazione che indicassero che questa e-mail in realtà non provenisse da WeTransfer. Tuttavia, erano presenti alcune impercettibili anomalie che Antigena Email è stato in grado di cogliere. Per prima cosa, la “percentuale di anomalia dell’Indirizzo IP” era elevata (63%). Questa metrica indica quanto insolito fosse per questo indirizzo di posta elettronica inviare e-mail da questo indirizzo IP, dato lo storico dei pattern di invio, ed è anche un’indicazione di uno spoof o di un account rubato.

Inoltre, poiché Antigena Email modella costantemente il comportamento “normale” di ogni mittente esterno affidabile, è riuscito a cogliere un’anomalia fondamentale nel testo dell’e-mail: un link incoerente, totalmente anomalo se confrontato con ciò che Darktrace ha rilevato in precedenza da WeTransfer. Questo contesto ha consentito ad Antigena Email di identificare il link come payload dannoso contenuto nell’e-mail.

Il link in questione era nascosto dietro dei pulsanti in numerose parti all’interno dell’e-mail, incluso un falso link “https://wetransfer. com/...” e il testo “Inquiry Sheet.xls”. Antigena aveva attribuito al link una percentuale di anomalia del 96%.

Questo incidente ha dimostrato come Antigena Email applica il rilevamento delle anomalie per identificare attacchi di phishing evoluti che sfruttano la familiarità di un sito web affidabile al fine di distribuire un link dannoso e ottenere numerosi punti di accesso all’interno dell’organizzazione.

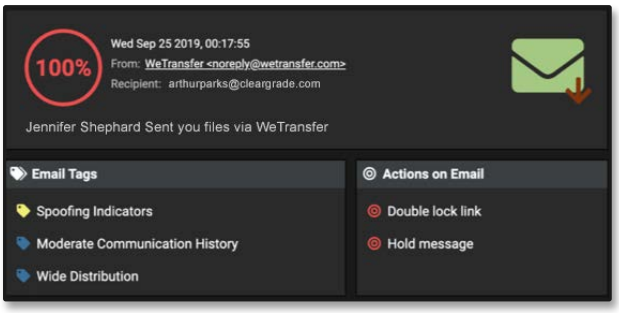

Figura 2: La user interface mostra i model breach e le azioni

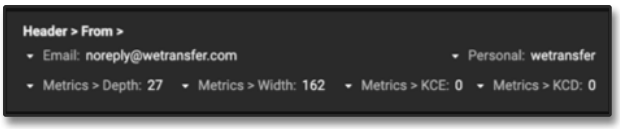

Figura 3: I dati di connessione delle e-mail rilevanti

Figura 4: Una scomposizione dei link mostrati nelle e-mail