

Email Security e Intelligenza Artificiale

I protection server non sono “onniscienti” e non sono in grado di comprendere il testo all’interno del body né di individuare qualunque tipo di minaccia.

Ad esempio, le email contenente solo testo (in cui si invita l’utente ad effettuare pagamenti e/o lo si minaccia) proveniente da domini molto utilizzati (come gmail, yahoo ecc) tendenzialmente non vengono bloccate in quanto il protection server non è in grado di comprendere il “significato” del testo di una mail. Quindi una mail proveniente da “pippo@gmail.com” contenente solo testo in cui si richiede un pagamento su un certo IBAN non è sempre detto che venga bloccata, anzi. In figura 10 è possibile osservare un tentativo di frode in cui si richiede un pagamento in bitcoin per evitare che venga diffuso materiale altamente personale del dipendente.



Figura 10. Mail malevola

Come si può evincere, la mail fa leva sullo stato emozionale che può scaturire sul destinatario. Realisticamente è probabile che non abbia nemmeno a disposizione il materiale di cui parla tuttavia tenta di creare panico nel dipendente che potrebbe, se non ha effettuato alcun tipo di training contro queste minacce, andare ad eseguire le azioni richieste.

Uno dei problemi principali quindi, oltre alla mancanza di training dei dipendenti, è legata alla mancanza da parte del secure gateway di bloccare queste tipologie di mail:

- sender proveniente da domini noti (gmail, yahoo e simili);
- mail contenente solo testo;

- nessuna evidenza malevola e/o di spoofing/phishing;

questo perché i mail secure gateway non sono “senzienti” e non sono quindi in grado di comprendere il testo. È in questo campo che si sta osservando l’entrata in gioco **dell’intelligenza artificiale (IA)**. Di fatto molti secure gateway moderni stanno iniziando ad integrare le IA nei loro sistemi allo scopo di bloccare e/o prevenire un maggior numero di minacce di questo tipo e non solo. Tra le IA più note ci sono **chatGTP** e **Gemini** ma se ne potrebbero citare molte altre in base all’ambito di interesse, tra cui Synthesia, Midjourney e Stable Diffusion.



Questo articolo è stato estratto dal white paper “Email Security: Intelligenza Artificiale, Protocolli e Best Practice Contro gli Attacchi Informatici” disponibile in maniera libera e gratuita al seguente link:
<https://www.ictsecuritymagazine.com/pubblicazioni/email-security-intelligenza-artificiale-protocolli-e-best-practice-contro-gli-attacchi-informatici/>

Articolo a cura di **Fabrizio Giorgione**

Profilo Autore



Fabrizio Giorgione è nato a Napoli (NA) nel 1992. Si è laureato in ingegneria informatica presso l’università degli studi del Sannio il 17 dicembre del 2018 con una tesi dal titolo: “Analisi della superficie di un sistema SCADA”. Ha sviluppato, presso il laboratorio ISWATlab, un’applicazione Android denominata “Privacy Guard” la quale valuta il rischio di privacy leakage, ovvero il furto di informazioni, sugli smartphone (http://www.iswatlab.eu/?page_id=499). Ha effettuato il tirocinio presso lo “ZLab” di “Cse Cyber Sec” nell’ambito “SOC”, “Forensic” e “Malware Analysis”. Attualmente lavora presso la società di “NTT DATA” come “Cyber

security Analyst” nel SOC di Napoli. Il suo compito è quello di effettuare analisi di log, di malware e di prevenire minacce interne ed esterne alla sua azienda e ai clienti della società. Si è occupato, inoltre, del montaggio e della gestione di sonde IDS/IPS presso Telecom Italia nella sede di Roma (RM).

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/email-security-e-intelligenza-artificiale/>