Gli attacchi via email continuano ad aumentare

Giu 26, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario 0

Il report di FireEye fotografa la tendenza del cyber-crimine. In aumento il phishing, l'uso di link "sicuri" e di servizi cloud di condivisione dei file.

Anche a distanza di anni, la posta elettronica è uno dei vettori di attacco più usati dai pirati informatici. A confermarlo è la nuova ricerca di **FireEye**, che nel suo **Email Threat Report** relativo al primo trimestre 2019 delinea le tendenze sulla base dell'analisi di **1.3 miliardi di email**.

Il primo dato che emerge dall'analisi, che conferma una tendenza rilevata nel corso degli ultimi anni, è quello dell'utilizzo del phishing come tecnica di attacco preferita da parte dei cyber-criminali. In termini numerici, l'incremento dell'uso di questa tecnica è del 17%.

La tendenza è quella di prendere di mira popolari servizi Internet, con l'obiettivo di rubare le credenziali delle potenziali vittime. Tra i servizi più gettonati ci sono quelli **Microsoft**, con circa il 30% di tutti i rilevamenti, seguita da **OneDrive**, **Apple**, **PayPal** e **Amazon**.

A segnare un aumento considerevole (+26%) è anche l'uso del protocollo HTTPS per gli attacchi basati sull'uso di url malevole. Qui la logica fa leva sul falso senso di sicurezza collegato al fatto che i collegamenti utilizzano un protocollo "sicuro".

Tra le novità c'è l'utilizzo di piattaforme cloud per il file sharing utilizzate per distribuire malware. I pirati utilizzano servizi noti come **WeTransfer**, **Google Drive** e **OneDrive**. Il primato in questo settore è però di **Dropbox**, considerato da molti come uno strumento "normale" per condividere file e documenti.

Non rallenta, infine, il fenomeno della BEC **(Business Email Compromise)** che prevede l'uso di attacchi mirati e tecniche di

social engineering attraverso i quali i pirati informatici impersonificano dirigenti delle aziende per disporre trasferimenti di denaro che finiscono nelle tasche dei cyber-criminali.

In questo settore, i ricercatori FireEye hanno individuato due nuove varianti rispetto allo schema “classico” di cui abbiamo parlato anche in passato.

La prima è **rivolta all’ufficio paghe di un’organizzazione** con un’email contenente una richiesta di modifica dei dati personali di un dirigente, come i dati bancari, con l’obiettivo di trasferire la retribuzione di un dirigente verso un conto di terzi.

La seconda, invece, colpisce il dipartimento che segue la contabilità dei fornitori dove gli attaccanti impersonano, tramite email, **un fornitore di fiducia** per reindirizzare un pagamento fraudolento verso un conto di terzi.

“Gli attaccanti stanno facendo i loro compiti. Stiamo assistendo a nuove varianti degli attacchi di

impersonificazione che mirano a nuovi contatti e nuovi dipartimenti all'interno delle organizzazioni" commenta **Ken Bagnall, Vice President of Email Security di FireEye**. "Il pericolo è che queste nuove vittime potrebbero non essere preparate o possedere le conoscenze necessarie per identificare un attacco. Sfortunatamente, una volta scoperta l'attività fraudolenta, l'organizzazione vittima ritiene di aver pagato una fattura legittima, anziché aver effettuato la transazione direttamente sul conto dell'attaccante".

Condividi l'articolo

Compagnie telefoniche hackerate per spiare gli utenti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/26/gli-attacchi-via-email-continuano-ad-aumentare/