Microsoft cerca di frenare i malware nei documenti Office

Giu 24, 2020 Marco Schiaffino In evidenza, News, Prodotto, RSS, Tecnologia 0

La nuova funzione si chiama Documenti Attendibili e dovrebbe consentire di ridurre il rischio di attacchi portati sfruttando i contenuti attivi.

Niente da fare: dopo più di 20 anni, i documenti **Office** rimangono uno dei vettori di attacco più utilizzati dai pirati informatici e, stando alle statistiche delle società di sicurezza, anche i più efficaci.

Microsoft, dopo aver introdotto nel corso del tempo modifiche di vario genere per mitigare il rischio di questa tipologia di attacchi, adesso prova un approccio diverso offrendo una nuova funzione nel suo pacchetto **Office 365**.

Si chiama **Documenti Attendibili** (**Safe Documents** nella versione inglese) e, in pratica, introduce un altro livello di controllo alla procedura di apertura dei file che hanno una provenienza potenzialmente sospetta.

Per la verità Office riserva già un trattamento particolare a tutti i documenti che provengono da Internet, come quelli allegati ai messaggi di posta elettronica. I file vengono aperti in **Visualizzazione Protetta**, cioè in una modalità "solo lettura". L'accesso completo per la modifica richiede una ulteriore conferma da parte dell'utente.

La logica di questo passaggio è legata al fatto che, in visualizzazione protetta, eventuali exploit contenuti nel documento non possono attivarsi.

Con Documenti Attendibili, la strategia si arricchisce di un ulteriore passaggio: il file viene aperto in visualizzazione protetta e, contemporaneamente, viene inviato al software di protezione **Microsoft Defender Advanced Threat Protection** (ATP) per un controllo approfondito.

Solo una volta verificata l’assenza di codice malevolo, il software propone la possibilità di abilitare la modifica del file.

La funzionalità, che ha superato una fase di rodaggio avviata nel febbraio scorso, è adesso disponibile per (quasi) tutti. Documenti Attendibili, infatti, è integrata nel pacchetto **Office 365 E5**, la versione più “accessoriata” (e costosa) del prodotto Microsoft.

Per impostazione predefinita, però, la funzione è disabilitata. Sarà quindi compito degli amministratori di sistema impostarne il funzionamento in modo che si attivi.

Condividi l’articolo

BlueLeaks: Anonymous negli USA “buca” i sistemi di polizia e FBI

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/06/24/office-documenti-attendibili/?utm_source=rss&utm_medium=rss&utm_campaign=office-documenti-attendibili