Falla in Microsoft Teams: l’account si ruba con una GIF

Apr 27, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La tecnica permette di sottrarre i dati dell’account utente attraverso una catena di azioni che sfruttano una vulnerabilità nell’autenticazione.

Non solo Zoom. Con il boom delle videoconferenze e dello smart working l’attenzione dei ricercatori di sicurezza si sta concentrando sulle piattaforme di comunicazione e collaborazione. Tra questi, un ruolo di primo piano, soprattutto a livello aziendale, l’ha **Microsoft Teams**.

La notizia della presenza di una vulnerabilità nella piattaforma di chat, videoconferenza e collaborazione basata su **Skype for Business** rappresenta quindi una pessima notizia per le aziende.

A individuare il problema sono stati i ricercatori di **CyberArk**, che in un (dettagliatissimo) report pubblicato sul blog ufficiale della società di sicurezza spiega come sia possibile sottrarre un account Microsoft Teams utilizzando una semplice immagine in formato **GIF**.

La possibilità di un attacco deriva da due fattori. Il primo è la modalità con cui vengono gestite le immagini e la loro visualizzazione in Teams. **Il secondo risiede nel sistema di autenticazione di Teams, che sfrutta un sistema di due token che vengono scambiati con i server Microsoft**.

Riassumendo: quando un’immagine viene inviata in Teams, è memorizzata sui server Microsoft e per guardarla è necessario

che il software si autentichi. I token utilizzati per l’autenticazione, che vengono generati volta per volta, possono essere però intercettati da chi gestisce dei sottodomini di teams.microsoft.com.

La domanda, qui, sorge spontanea: è possibile che un pirata informatico ottenga il controllo di un sottodominio del genere? Secondo i ricercatori di CyberArk, sì. In particolare, gli analisti della società di sicurezza ne hanno potuti individuati rapidamente due: **aadsync-test.teams.microsoft.com** e **data-dev.teams.microsoft.com**.

Come funzionerebbe quindi l’attacco? Lo schema qui sotto lo spiega bene.

Dopo essersi assicurato il controllo di un sottodominio adeguato, il pirata informatico non deve fare altro che inviare un messaggio con una GIF creata ad hoc che gli consente di recuperare i token di autenticazione e rubare l’accesso all’account della vittima.

A questo punto, può usare l’account rubato per inviare il messaggio ad altri utenti all’interno dell’azienda e sottrarre così tutti i messaggi e i dati scambiati con Microsoft Teams.

Il tutto avverrebbe senza alcun segnale che possa far pensare a una violazione e avrebbe quindi un impatto devastante.

La vulnerabilità, comunicata tempestivamente a Redmond, è stata corretta con un aggiornamento del software e adesso il rischio di un furto di account tramite l'invio di immagini. Tutta la vicenda, però, rappresenta un ulteriore indizio di quanto i sistemi di comunicazione e collaborazione siano vulnerabili ad attacchi esterni.

Condividi l'articolo

Allarme dell'NSA sulla diffusione delle Web Shell

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/27/falla-in-microsoft-teams-laccount-si-ruba-con-una-gif/?utm_source=rss&utm_medium=rss&utm_campaign=falla-in-microsoft-teams-laccount-si-ruba-con-una-gif