BlackDirect espone alla violazione degli account Microsoft Azure

Dic 05, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il sistema di autenticazione usato da Microsoft lascia aperta la strada a un attacco che potrebbe consentire il furto dell'account.

È stata battezzata con il nome i **BlackDirect** ed è una tecnica di attacco che permette di eseguire operazioni con elevati privilegi di amministrazione sugli account **Microsoft Azure**.

A individuare la falla di sicurezza sono stati i ricercatori di **CyberArk**, che ne descrivono i dettagli in un report pubblicato sul sito ufficiale della società di sicurezza.

Ma di cosa si tratta nel dettaglio? Tutto prende le mosse da **OAuth 2**, la nuova versione del sistema di autenticazione utilizzato dai sistemi Microsoft. OAuth, infatti, prevede la possibilità di prevedere una forma di interazione che permette di eseguire l'accesso da un'applicazione di terze parti.

La procedura è gestita attraverso la creazione di un **token** che, in pratica, garantisce l'utilizzo delle funzionalità legate all'account.

Come spiega **Omer Tsarfati**, autore del report,, il sistema in sé è strutturato in maniera solida e quello individuato da CyberArk non è una vulnerabilità di OAuth, quanto un problema legato a un'impostazione "debole" delle procedure che sfruttano il sistema di autenticazione.

Le terze parti autorizzate a eseguire l'accesso attraverso il redirect comprendono infatti URL definite attraverso una white list che elenca i domini e i sottodomini a cui è consentito utilizzare OAuth. Alcuni di questi, fanno notare i ricercatori, non sono registrati da Microsoft e potrebbero, di conseguenza, rappresentare un fattore di rischio.

Se un pirata informatico riuscisse a prenderne il controllo, potrebbe infatti sfruttare il sistema di autenticazione attraverso token per eseguire operazioni come se fosse il legittimo proprietario dell'account.

Per mettere a segno l'attacco, sarebbe sufficiente attirare la vittima sul sito Web attraverso tecniche di social engineering, per esempio attraverso un semplice messaggio di posta elettronica.

Il problema è che ci sono almeno tre applicazioni Microsoft che prevedono, all'interno della lista, una serie di domini che i ricercatori considerano "a rischio". Si tratta di **Portfolios**, **O365 Secure Score** e **Microsoft Service Trust**. In seguito alla segnalazione di CyberArk, Microsoft ha corretto il problema.

Per quanto riguarda invece altre applicazioni, è possibile eseguire un controllo attraverso uno strumento sviluppato dalla stessa società di sicurezza e che può essere utilizzato gratuitamente attraverso la pagina Web dedicata

https://black.direct/.

Condividi l’articolo

Hacker tentano un attacco 51% contro Vertcoin, ma ci perdono soldi

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/05/blackdirect-espone-alla-violazione-degli-account-microsoft-azure/