Attacco a un server MDM per diffondere un malware per Android

Mag 04, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L'azione mirata ha permesso ai pirati di prendere il controllo del sistema di Mobile Device Management e distribuire il trojan Cerberus.

L'adozione di sistemi di **Mobile Device Management (MDM)** rappresentano uno strumento fondamentale attraverso il quale le aziende possono garantire un adeguato livello di sicurezza sui dispositivi mobili dei loro dipendenti, prevedendo la distribuzione centralizzata di aggiornamenti e il controllo dei software di protezione.

Come ogni sistema centralizzato, però, MDM rappresenta un bersaglio ideale per i pirati informatici, che potrebbero sfruttarlo per colpire con facilità un elevato numero di dispositivi sfruttando un canale privilegiato.

Fino a oggi, però, questa era solo un'ipotesi. Ora non più. Come spiegano i ricercatori di **Check Point**, il primo caso di violazione di un sistema MDM è stato compiuto da un gruppo di pirati informatici che hanno sfruttato la tecnica per diffondere **Cerberus**, un trojan per smartphone **Android**.

Nel loro report, gli analisti della società di sicurezza ricostruiscono la vicenda partendo dal rilevamento di una inusuale diffusione del malware che ha insospettito da subito gli esperti.

L’azienda colpita, di cui non indicano il nome, ha infatti subito un attacco che ha portato in pochissimo tempo all’infezione del 75% dei dispositivi mobili aziendali.

Un fenomeno che ha fatto pensare a due ipotesi: l’utilizzo di un malware in grado di diffondersi attraverso una sorta di “movimento laterale” all’interno della rete mobile dell’azienda o, appunto, la compromissione del sistema MDM.

L’azienda interessata ha confermato la seconda ipotesi, senza fornire però maggiori dettagli sulle modalità con cui i cyber-criminali avrebbero preso il controllo del sistema.

Anche se derivato da un malware originariamente specializzato nel furto delle credenziali dei servizi bancari, Cerberus è un classico trojan programmato per sottrarre informazioni personali e, in particolare, le credenziali di accesso a servizi, gli SMS e il registro delle chiamate.

L’obiettivo dei pirati informatici, quindi, era presumibilmente quello di avviare una campagna di spionaggio in grande stile ai danni dell’impresa colpita.

Condividi l’articolo

Boom di attacchi ai collegamenti in remoto RDP

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/04/attacco-a-un-server-mdm-per-diffondere-un-malware-per-android/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-a-un-server-mdm-per-diffondere-un-malware-per-android