Attacchi a Windows e Android sfruttavano falle zero-day

Gen 13, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Il report di Google esamina le tecniche di un gruppo di pirati che sfruttavano una complessa concatenazione di bug per portare i loro attacchi.

Un complesso sistema per portare attacchi informatici è stato descritto un corposo report (pubblicato in sei parti) da parte dei ricercatori di sicurezza del **Project Zero Team** di **Google**.

Lo studio (qui il collegamento alla prima parte) si riferisce a una campagna di attacchi che i ricercatori hanno individuato all'inizio del 2020 e che sfruttava una serie di bug in **Chrome**, **Windows** e **Android**.

I cyber criminali utilizzavano dei server dedicati per utilizzare i loro exploit, attirando presumibilmente le vittime su pagine Web che avevano compromesso.

Gli exploit, inseriti attraverso **due iFrame separati**, consentivano di sfruttare una serie di vulnerabilità (alcune delle quali al tempo dell'individuazione erano ancora sconosciute) per installare trojan sui dispositivi Windows e Android delle vittime.

Il punto di partenza erano **nove vulnerabilità del sistema di rendering del browser Chrome**, quattro delle quali zero-day, che venivano combinate allo sfruttamento di tecniche di **sandbox escape**, queste ultime rese possibili da ulteriori bug nelle due piattaforme.

Le falle di sicurezza, che sono state corrette nel corso dell'anno passato, venivano sfruttate attraverso una catena di exploit estremamente elaborata e che i ricercatori di Google ritengono essere stata creata da soggetti con un'elevata professionalità.

L'ecosistema creato dai pirati informatici consentiva, in pratica, di utilizzare le stesse pagine Web per colpire sia i PC con sistema Windows, sia gli smartphone Android. Obiettivo finale: installare su di essi un "impianto" (un trojan) in grado di sottrarre informazioni dai dispositivi compromessi.

Una strategia che, abbinata all'elevata complessità della tecnica di attacco, fa immediatamente pensare all'azione di un gruppo APT. Sull'identità o la nazionalità dei pirati, però, il report non si sbilancia.

Condividi l'articolo

Corretto bug in Microsoft Defender, ma i pirati lo stavano già usando

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/01/13/attacchi-a-windows-e-android-sfruttavano-falle-zero-day/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-a-windows-e-android-sfruttavano-falle-zero-day