Comunicato stampa
For immediate release
Mercoledì, 31 maggio 2023

Contatti: Alina Anton
T +40 726 366703
E aanton@bitdefender.com

Scoperte 60.000 app Android infettate da malware

Lo rivela una ricercar Bitdefender che avverte gli utenti su come lo scopo della campagna sia quello di diffondere adware, Trojan bancari e ransomware sui dispositivi Android per generare profitti

Milano, 8 giugno 2023 - Bitdefender pubblica oggi una nuova ricerca su una massiccia campagna di malware che ha preso di mira le applicazioni Android e che è rimasta inosservata per almeno sei mesi: finora sono state identificate **60.000 app dannose** (in costante crescita) che utilizzano tecniche per passare inosservate e indurre gli utenti a installarle con lo **scopo di diffondere adware, Trojan bancari e ransomware sui dispositivi Android per generare profitti.**

La campagna coinvolge principalmente coloro che installano app da fonti diverse da Google Play e che sono alla ricerca di applicazioni "moddate" per giochi popolari e **servizi come YouTube, Netflix, TikTok, software di sicurezza contraffatti, VPN gratuite, tutorial falsi, applicazioni di pubblica utilità come per esempio il meteo** o visualizzatore di pdf e altri. Di solito, le applicazioni moddate sono applicazioni originali modificate con tutte le loro funzionalità sbloccate o con modifiche alla programmazione iniziale.

Questa scoperta è stata resa possibile da una nuova tecnologia recentemente introdotta da Bitdefender, denominata App Anomaly, che utilizza modelli di machine learning per rilevare comportamenti sospetti delle app anche dopo l'installazione sui dispositivi.

Risultati principali:

- I criminali informatici hanno bisogno di convincere gli utenti a scaricare le app dannose, quindi camuffano queste applicazioni da app diffuse o prodotti ricercati che non si trovano sullo store Google Play ufficiale.
- Nel momento in cui l'utente cerca di installare l'app viene visualizzato un messaggio di errore che induce l'utente a pensare che l'installazione non sia andata a buon fine, mentre in realtà l'app dannosa è nascosta nel sistema, elencata solo nella sezione Impostazioni > Info app, sempre alla fine dell'elenco, senza nome e con un'icona vuota.
- La tecnica dei messaggi di errore, abbinata a un ritardo temporale appositamente creato per le attività dannose, rende estremamente difficile il rilevamento.

- Ad esempio, un meccanismo tipico di questa campagna si verifica quando l'utente apre un sito Web da una ricerca su Google di un'applicazione "moddata" e viene reindirizzato a una pagina pubblicitaria casuale. A volte, quella pagina è una pagina di download di malware mascherata da download legittimo dell'app moddata che l'utente stava cercando.
- Gli Stati Uniti sono il paese più bersagliato con il 55%, seguiti dalla Corea del Sud con il 9,8%. La campagna al momento colpisce solo marginalmente l'Europa: Regno Unito (2,71%) Francia (2,56%) e Italia (1,93%), ma Bitdefender invita tutti gli utenti a stare allerta perchè la scelta degli obiettivi potrebbe rapidamente cambiare.

Gli attacchi che colpiscono i dispositivi mobili stanno diventando sempre più frequenti e sofisticati. Bitdefender invita i consumatori e le aziende a stare attenti quando scaricano applicazioni e suggerisce di scaricare solo da fonti affidabili e di utilizzare una protezione antimalware su tutti i dispositivi.

Informazioni su Bitdefender

Bitdefender è una società leader nella sicurezza informatica che offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce del mondo. Proteggendo milioni di consumatori, aziende e ambienti governativi, Bitdefender è considerata uno degli esperti più affidabili del settore per eliminare le minacce, proteggere la privacy e i dati, e ottenere la resilienza informatica. Grazie a notevoli investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida miliardi di query sulle minacce al giorno. L'azienda ha aperto la strada a innovazioni rivoluzionarie in varie tecnologie, come anti-malware, sicurezza IoT, analisi comportamentale e intelligenza artificiale. La sua tecnologia è usata su licenza da più di 180 dei marchi tecnologici più noti al mondo. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo. Per maggiori informazioni, visitare https://www.bitdefender.it.

Per ulteriori informazioni

Prima Pagina Comunicazione

02/91339820

Tania Acerbi, Monica Fecchio, Elisa Pagano

tania@primapagina.it

monica@primapagina.it

elisa@primapagina.it