System Update

Si chiama System Update ma non è un aggiornamento di sistema, bensì un'app fake

dietro la quale si nasconde un potente spyware capace di prendere il pieno controllo dei dispositivi Android.

Il malware è infatti capace di rubare informazioni personali delle vittime: elenco dei contatti, segnalibri e cronologia del browser e messaggi WhatsApp; oltre ad essere in grado di registrare l'audio ambientale e le telefonate o di scattare foto utilizzando la fotocamera dello smartphone.

Inoltre, può anche tracciare la posizione della vittima, cercare file con estensioni specifiche ed esfiltrare dati dagli appunti del dispositivo.

L'app System Update non è presente all'interno del Google Play Store, ma può essere scaricata da fonti esterne e store di terze parti, che quindi si confermano ancora una volta pericolose fonti di diffusione di malware. Il nuovo spyware System Update rappresenta un'evoluzione rispetto agli altri malware per Android diffusi finora mediante la tecnica del copycat, cioè "mascherati" da popolari app per il sistema operativo di Google.

Un utente meno esperto potrebbe facilmente scambiare System Update per un importante aggiornamento del proprio smartphone e acconsentire quindi all'installazione dell'app malevola.

Secondo quanto analizzato dai ricercatori di sicurezza di Zimperium, una volta che la vittima installa l'app System Update, il malware comunica con un server attivo sulla piattaforma Firebase utilizzato per controllare da remoto il dispositivo compromesso.

Proprio grazie allo sfruttamento del servizio di messaggistica della piattaforma Firebase (di proprietà della stessa Google) lo spyware System Update è in grado di visualizzare una notifica sul dispositivo della vittima nel caso in cui lo schermo risultasse spento, per informarlo della disponibilità di un aggiornamento di sistema.

Completata l'installazione, lo spyware System Update avvia la sua campagna malevola registrando innanzitutto il dispositivo sul server di comando e controllo (C2) sulla piattaforma Firebase gestito dai cyber criminali. In questa fase, vengono inviate informazioni come la percentuale di carica della batteria, le statistiche sullo spazio di archiviazione nella memoria dello smartphone e se sul dispositivo è installato WhatsApp, il tutto sottoforma di un file ZIP crittografato.

Nel tentativo di eludere il rilevamento da parte di eventuali sistemi di controllo installati sullo smartphone target, il malware non solo organizza i dati raccolti in diverse cartelle all'interno della sua memoria privata, ma elimina anche qualsiasi traccia di attività dannosa cancellando i file ZIP non appena riceve un messaggio di avvenuta esfiltrazione dati dal server C2. Inoltre, per ridurre ulteriormente il rischio di essere identificato, lo spyware System Update riduce la quantità di traffico consumata caricando sul server C2 miniature delle immagini e anteprime dei video rubati alla vittima.

I consigli per mitigare i rischi

Secondo il CEO di Zimperium, Shridhar Mittal, "questo è senza dubbio lo spyware più sofisticato che abbiamo visto e penso sia stato speso molto tempo e impegno per crearlo. Crediamo che esistano altre app come questa e stiamo facendo del nostro meglio per trovarle e isolarle il prima possibile".

L’analisi dello spyware System Update conferma, inoltre, come ingannare qualcuno a installare un’ app dannosa rappresenti un modo semplice ma efficace per compromettere il dispositivo di una vittima mirata. Per questo motivo è importante evitare di installare app al di fuori del Google Play Store, a meno di non avere la certezza assoluta sulla sua autenticità.

Il problema è che su molti vecchi dispositivi non è possibile eseguire le versioni più recenti delle app usate quotidianamente e questo spinge molti utenti a scaricare vecchie versioni ancora compatibili con il proprio smartphone da app store illegali o non attendibili.

Fortunatamente, come abbiamo visto, lo spyware nascosto nella finta app System Update richiede l’azione dell’utente per essere installato: alla luce di quanto appena detto, il consiglio è dunque quello di non installare file APK scaricati da fonti non attendibili.

Anche alla luce del fatto che l’identità degli autori del malware, le vittime mirate e il motivo finale della campagna malevola rimangono ancora poco chiari.