Agent Smith: il nuovo malware per Android fa strage di smartphone

Lug 11, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

Si nasconde sullo smartphone e modifica le applicazioni installate per bombardare la vittima di pubblicità. Già colpiti 25 milioni di dispositivi.

Si chiama **Agent Smith** il nuovo spauracchio che si aggira per la rete e che colpisce i dispositivi Android per intasarli di pubblicità indesiderate.

Il malware sarebbe comparso su alcuni store di terze parti, infettando la bellezza di **25 milioni di dispositivi Android**. Secondo **Check Point**, che descrive le caratteristiche del malware in un report sul suo sito Internet, il primo "focolaio" sarebbe stato **9Apps**, uno store Android molto usato in India.

Il malware, contenuto all'interno di applicazioni gratuite e giochi per smartphone, agisce in maniera particolarmente insidiosa. Il codice del modulo principale è crittografato all'interno di un'immagine JPEG.

Una volta installata l’applicazione, il codice del malware viene estratto e avviato sullo smartphone sfruttando una serie di vulnerabilità conosciute che consentono la sua installazione senza che sia necessaria alcuna interazione da parte dell’utente.

Agent Smith si “mimetizza” per sembrare **un’applicazione di Google** e nasconde la sua icona in modo che la vittima non riesca a individuarne la presenza. I nomi utilizzati possono cambiare, ma sono sempre del tipo “Google Updater” o “Google Update for U”.

In una seconda fase, il malware si collega al server Command and Control e, subito dopo, controlla l’elenco delle applicazioni installate sullo smartphone alla ricerca di alcune app di uso comune, come **Whatsapp.**

Utilizza poi una vulnerabilità conosciuta come Janus, che permette di sostituire le applicazioni legittime con una versione malevola, al cui interno è presente il modulo che gestisce la visualizzazione di pubblicità indesiderate sul

telefono.

Una volta completata la sua opera, il malware deve solo preoccuparsi di garantire la persistenza delle applicazioni “modificate”. Per farlo, evita che possano eseguire gli aggiornamenti da parte del legittimo sistema di update.

I trucchi utilizzati sono due. Il primo è un sistema di monitoraggio che controlla costantemente la directory dedicata agli aggiornamenti e cancella immediatamente qualsiasi file di installazione compaia al suo interno.

Il secondo, invece, impatta sul sistema che gestisce il controllo degli aggiornamenti per fare in modo che l’applicazione non abbia scadenze per il controllo.

Oltre alle caratteristiche tecniche, i ricercatori di Check Point sottolineano nel loro report il fatto che la campagna di attacchi avviata da questo gruppo di pirati informatici è estremamente aggressiva. Analizzando lo store 9Apps, gli esperti hanno infatti individuato **più di 360 varianti del dropper**.

Non solo: l’elenco delle applicazioni che Agent Smith prende di mira è estremamente ampio. Secondo le analisi della società di sicurezza, i 25 milioni di dispositivi infetti conterrebbero in totale **2,8 miliardi di app “modificate”**. Una

media di 112 per dispositivo.

Le preoccupazioni, però, riguardano anche altri aspetti. Secondo quanto si legge nel report, infatti, gli autori del malware starebbero pianificando un attacco che prenderebbe di mira direttamente **Google Play**. Gli esperti di Check Point, infatti, hanno individuato **11 app nello store ufficiale di Google** che contengono una versione "dormiente" del malware.

Il vero rischio, però, è che Agent Smith possa evolvere in maniera ancora più preoccupante. La struttura modulare del malware, infatti, permette di introdurre qualsiasi tipo di funzionalità. **In futuro potremmo assistere alla comparsa di varianti con obiettivi decisamente più nocivi rispetto alla semplice visualizzazione di messaggi pubblicitari**.

Ma chi c'è dietro questo attacco? Dalle indagini dei ricercatori emerge un collegamento con una società cinese con sede a **Guangzhou**, che opera alla luce del sole, proponendo servizi di assistenza per gli sviluppatori Android che vogliono pubblicare le loro app sulle piattaforme estere. In pratica, una copertura perfetta.

Condividi l'articolo

Ecco come ti rubo i file con un bug di Firefox

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/11/agent-smith-il-nuovo-malware-per-android-fa-strage/