Joker, come funziona il malware Android che elude la sicurezza di Google

Apparso in natura per la prima volta nel 2017, il **malware Joker**, ovvero uno spyware sofisticato concepito per commettere frodi informatiche è stato nuovamente individuato dai ricercatori di **Check Point Research** in nuova variante.

Il malware Joker

Questa volta, continuando a eludere i sistemi di protezione dello Store di **Google**, ha agito per fare attivare servizi a pagamento alle vittime ignare colpite, celandosi in modo subdolo in ben 11 app.

Figura: Una delle app/Joker rilevate su Google Play Store da Chek Point Research

La tecnica di offuscamento

Nel tentativo di offuscare l'impronta digitale di Joker, i criminal hacker hanno nascosto il caricamento dinamico del file .dex, file di inizializzazione previsto dai sistemi Android, pur garantendone il download attraverso una strategia simile a quella ben nota agli sviluppatori di malware per PC Windows.

In questa nuova veste, infatti, il codice dannoso del malware,

noto anche con il nome di Bread, si nascondeva, come file “dex” sotto forma di stringhe codificate in Base64, all’interno del cosiddetto file di progetto xml “AndroidManifest” che ogni app deve contenere nella sua directory principale, per fornire al sistema ospitante determinate informazioni essenziali per una corretta esecuzione del codice.

Con questo escamotage i criminal hacker sono riusciti, così, ad evitare l’accesso ad un server C2 per inviare comandi ai sistemi compromessi e scaricare definitivamente il payload, azioni che sarebbero state di sicuro captate dalle ultime routine di sicurezza adottate da Google.

La catena d’infezione

Come spiegato dagli stessi analisti, gli sviluppatori criminali in questa versione del malware hanno implementato un processo d’infezione suddiviso in tre fasi, sempre allo scopo di migliorarne l’offuscamento e l’invisibilità, arginando così scrupolosamente i controlli di sicurezza che il Play Protect Google aggiorna periodicamente:

1. **creazione del payload**: il payload viene inserito nel file “Android Manifest”;
2. **attesa per il caricamento del payload**: durante tutto il tempo necessario per il processo di valutazione dell’app, Joker resta dormiente per bypassare le protezioni di Google Play Store;
3. **diffusione del payload**: cessato il periodo di valutazione e dopo l’avvenuta approvazione dell’app, Joker si attiva e il payload viene caricato sul dispositivo dell’ignara vittima.

Come difendersi

In questi ultimi anni, il malware Joker con le sue varianti,

come confermato dalla stessa Google, è riuscito, tramite diverse tecniche di cloaking, a mascherare il proprio contenuto malevolo celandosi in applicazioni apparentemente legittime, diventando, di fatto, una delle più gravi minacce persistenti del suo genere.

Alla luce di quanto detto, poiché non si può escludere che Joker torni a far danno sotto altre mentite spoglie e qualora si dovesse sospettare di avere installato una di queste app sul proprio dispositivo, è di fondamentale importanza:

- disinstallare l'app presumibilmente infetta;
- controllare le liste movimenti di carte di pagamento e del credito residuo smartphone presso il proprio gestore telefonico, controllando che non siano stati attivati eventuali abbonamenti anomali;
- prevenire future infezioni proteggendo il proprio smartphone con una soluzione di protezione adeguata.

I ricercatori di sicurezza hanno ovviamente divulgato la scoperta in modo responsabile a Google e già dallo scorso 30 aprile le app segnalate risultano rimosse dal Play Store. Di seguito si riportano gli IoC dei *package* resi pubblici.

https://www.key4biz.it/joker-come-funziona-il-malware-android-che-elude-la-sicurezza-di-google/313726/