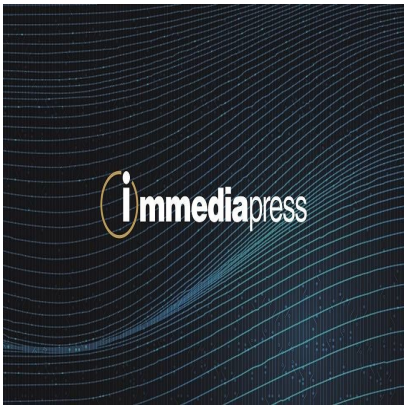

Kaspersky scopre una nuova campagna malware per Android che si nasconde dietro unâ??applicazione Starlink

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Il Global Research and Analysis Team (GReAT) di Kaspersky ha scoperto una nuova campagna malware per Android in cui i criminali informatici hanno distribuito il trojan BeatBanker sotto le spoglie dellâ??applicazione Starlink per Android. Gli autori delle minacce prendono di mira principalmente gli utenti brasiliani, ma gli esperti di Kaspersky non escludono che anche gli utenti di altri Paesi possano essere esposti a questa minaccia.

Il trojan utilizza un miner di criptovaluta Monero e installa inoltre uno strumento di amministrazione remota (RAT) BTMOB sui dispositivi infetti. Per mantenere la persistenza, BeatBanker utilizza un meccanismo insolito che coinvolge un file audio riprodotto in loop quasi impercettibile.

â?• Inizialmente abbiamo osservato BeatBanker distribuito sotto le spoglie di unâ??app di servizi pubblici: oltre a un miner di criptovalute, installava anche un trojan bancario. Tuttavia, i nostri recenti sforzi di rilevamento hanno portato alla luce una nuova campagna con unâ??altra variante di BeatBanker, che distribuisce il RAT BTMOB invece del modulo bancario. Gli aggressori sembrano utilizzare una nuova esca, lâ??app Starlink, per raggiungere piÃ¹ vittime in diversi Paesi. Per questo motivo Ã¨ importante che gli utenti prestino attenzione e utilizzino soluzioni avanzate per proteggere i propri smartphoneâ?•, ha commentato Fabio Assolini, Head of the Americas & Europe Units di Kaspersky GReAT.

Vettore iniziale dellâ??infezione

Gli esperti di Kaspersky ritengono che i criminali informatici distribuiscano una falsa applicazione Starlink contenente il trojan BeatBanker attraverso pagine di phishing che imitano il Google Play Store. Dopo lâ??esecuzione su un dispositivo compromesso, il trojan visualizza unâ??interfaccia utente che imita anchâ??essa Google Play. I criminali informatici inducono cosÃ¬ le vittime a concedere i permessi di installazione, consentendo il download di ulteriori payload dannosi nascosti.

Crypto mining e modulo RAT BTMOB

Quando un utente clicca su AGGIORNA nella falsa pagina di Google Play, viene installato un miner di criptovaluta Monero. BeatBanker monitora la percentuale di batteria, la temperatura dello smartphone infetto e lâ??attivitÃ dellâ??utente, avviando o arrestando di conseguenza un miner di criptovaluta nascosto.

Il trojan Android installa inoltre un BTMOB RAT sul dispositivo compromesso. BTMOB consente il controllo remoto completo ed Ã¨ venduto come Malware-as-a-Service. Ã? in grado di concedere automaticamente le autorizzazioni, nascondere le notifiche di sistema e dispone di meccanismi progettati per acquisire le credenziali di blocco dello schermo, inclusi PIN, sequenze e password sui dispositivi compromessi. Il malware consente inoltre ai criminali di accedere alle fotocamere anteriori e posteriori, monitorare la posizione GPS e raccogliere costantemente dati sensibili.

Per garantire la persistenza e impedire la disinstallazione, BeatBanker mantiene una notifica fissa in primo piano e attiva un servizio in foreground con riproduzione multimediale silenziosa. Questa tattica Ã¨ progettata per impedire al sistema operativo di rimuovere il processo dannoso.

I prodotti Kaspersky rilevano questa minaccia come HEUR:Trojan-Dropper.AndroidOS.BeatBanker e HEUR:Trojan-Dropper.AndroidOS.Banker.*.

Per ulteriori informazioni Ã¨ possibile consultare il report su Securelist.

Per proteggersi dalle minacce mobile, Kaspersky raccomanda di:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Marzo 10, 2026
Autore
redazione