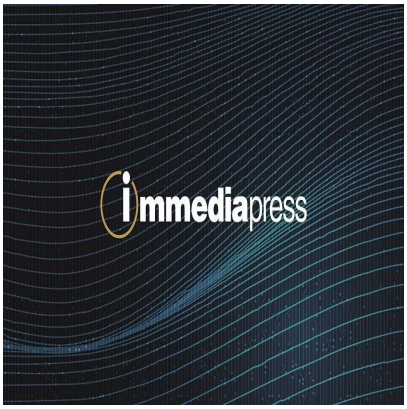

Kaspersky identifica lâ??exploit Coruna come evoluzione del framework Operation Triangulation

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Il Global Research and Analysis Team (GReAT) di Kaspersky ha condotto unâ??analisi a livello di codice degli exploit Coruna, stabilendo che il kit rappresenta una versione aggiornata e diretta del framework utilizzato, almeno in parte, nella campagna di spionaggio informatico denominata â??Operation Triangulationâ?•. Kaspersky ritiene che gli exploit del kernel presenti sia in Triangulation sia in Coruna siano stati sviluppati dallo stesso autore.

Lâ??analisi ha inoltre rivelato che uno dei cinque exploit del kernel inclusi nel kit Ã¨ una versione aggiornata dello stesso exploit scoperto da Kaspersky durante Operation Triangulation nel 2023. I restanti quattro, tra cui due sviluppati dopo la divulgazione pubblica di Operation Triangulation, si basano sul medesimo framework. Le somiglianze nel codice non si limitano agli exploit del kernel, ma si estendono anche ad altri componenti di Coruna, portando Kaspersky a concludere che il kit non Ã¨ composto da elementi eterogenei, bensÃ¬ rappresenta unâ??evoluzione costante del framework originale.

Il codice include il supporto per i processori Apple A17, M3, M3 Pro e M3 Max, oltre a riferimenti alle versioni di iOS fino alla 17.2, tutte rilasciate tra lâ??autunno e lâ??inverno del 2023. Ã? inoltre presente un controllo specifico per iOS 16.5 beta 4, la versione distribuita da Apple per correggere le vulnerabilitÃ segnalate da Kaspersky.

â??Quando Coruna Ã¨ stata segnalata per la prima volta, le prove disponibili non erano sufficienti per collegarne il codice a Triangulation: la semplice presenza di vulnerabilitÃ condivisa non dimostra, di

per sÃ©, una responsabilitÃ condivisa. Ora che abbiamo analizzato i file binari effettivi, il quadro Ã¨ cambiato. Coruna non Ã¨ un mosaico di exploit pubblici, ma unâ??evoluzione costantemente aggiornata del framework originale di Operation Triangulation. Lâ??inclusione di controlli per processori recenti come lâ??M3 e per le versioni piÃ¹ recenti di iOS dimostra che gli sviluppatori originali hanno continuato ad ampliare attivamente questo codice base. Quello che era nato come uno strumento di spionaggio di precisione viene ora utilizzato in modo indiscriminato â??, ha dichiarato Boris Larin, Principal Security Researcher di Kaspersky GReAT.

Kaspersky invita tutti gli utenti iPhone a installare immediatamente gli ultimi aggiornamenti di iOS. Sebbene le vulnerabilitÃ sfruttate da Coruna siano state corrette da Apple, i dispositivi che non hanno ancora installato gli aggiornamenti restano esposti a rischi.

Lâ??analisi tecnica completa Ã¨ disponibile su Securelist.com.

Operation Triangulation Ã¨ una campagna di Advanced Persistent Threat (APT) rivolta ai dispositivi iOS, resa nota per la prima volta nel giugno 2023. Kaspersky ha individuato la campagna monitorando il traffico di rete della propria rete Wi-Fi aziendale: lâ??attore malevolo aveva preso di mira i dispositivi iOS di decine di dipendenti. I ricercatori hanno identificato quattro vulnerabilitÃ zero-day sfruttate nella campagna, che interessavano unâ??ampia gamma di prodotti Apple.

Per proteggersi da attacchi mirati, condotti da attori noti o sconosciuti, i ricercatori di Kaspersky raccomandano 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 30, 2026
Autore
redazione