Il Sole 24 ORE

Cybersecurity: davvero iPhone e i dispositivi Apple sono ancora a prova di hacker?

—di **Giancarlo Calzetta** | 29 agosto 2018

Apple ha sempre puntato molto sul comunicare agli utenti che i propri sistemi siano più sicuri rispetto a quelli della concorrenza, ma i tempi stanno cambiando e gli hacker che impegnano il loro tempo nel cercare vulnerabilità per comunicarle alle aziende sono molto preoccupati.

Durante l'ultimo Black Hat, una convention di hacker che si tiene a Las Vegas**, il ricercatore Ian Beer ha tenuto un discorso mettendo nel mirino le politiche di Apple** e di altri grandi produttori quando si tratta di risolvere le vulnerabilità.

Ian Beer fa parte del team Project Zero, una squadra di hacker che Google ha creato proprio con il proposito di cercare vulnerabilità e comunicarle ai produttori per rendere più sicuro il settore e sensibilizzarli al problema degli attacchi informatici. Ebbene, Beer **lamenta il fatto che nonostante questi ultimi siano piuttosto pronti a emettere delle patch, sono estremamente riluttanti ad andare a cercare soluzioni definitive ai bug segnalati, limitandosi a fare il compitino per risolvere il problema in superficie.**

Il problema, secondo Beer, non sono gli specialisti di sicurezza, ma l'atteggiamento di chi sta a capo del dipartimento, i quali avendo una formazione accademica, e non da 'hacker' in senso stretto, non hanno la sensibilità necessaria ad andare alla radice dei problemi, lasciando nel codice le basi per lo sfruttamento del bug in modi diversi da quello segnalato.

«Sicuramente – dice Beer – queste persone hanno delle competenze molto elevate nel campo della sicurezza informatica, ma non hanno un passato di ricerca nello sfruttamento delle vulnerabilità...»

Questo limita grandemente il loro operato e Beer sostiene che non si fanno quelle domande che poi portano gli hacker a violare i sistemi: "perché questo bug è qui? Come può essere usato? Perché non lo abbiamo visto prima?" e così via.

Fino a qualche anno fa, Apple poteva contare sul fatto che, in fondo, i criminali preferivano attaccare i sistemi Windows che sono molto più diffusi per arrivare ai loro scopi. Con il diffondersi degli attacchi mirati, però, le cose stanno cambiando e il malware per iOS e MacOS sta diventando molto comune negli attacchi.

Ai primi di agosto, Amnesty International ha dichiarato di esser stata oggetto di una campagna di spionaggio che sfruttava proprio un malware per iOS che si chiama Pegasus, prodotto da un'azienda di "sicurezza" israeliana. Lo stesso malware sembra esser stato usato in una campagna che andava a minare una iniziativa messicana per promuovere una legge anti obesità.

«Strumenti come Pegasus – dice Beer – una volta erano usati solo dai governi, ma adesso sembra che sia a portata delle aziende che vendono bibite zuccherate».

Analogamente, **Kaspersky Lab ha riportato un caso di violazione di un CryptoExchange, un'azienda che permette agli utenti di comprare, vendere e conservare criptovalute come i bitcoin, che è avvenuta grazie un malware per Mac** scritto, con probabilità, da un gruppo di hacker della Corea del Nord.

Beer indirizza le sue parole particolarmente verso Apple perché ha dedicato molto tempo all'analisi dei sistemi della mela morsicata e li conosce molto bene, ma il suo discorso deve essere applicato a tutti i

produttori.
Secondo lui deve finire il tempo in cui si produce un patch superficiale per chiudere il problema segnalato e si deve andare a fondo della struttura dei software in cui si segnalano vulnerabilità per risolvere il problema a livello di design e non solo per dare agli utenti la falsa sensazione che la sicurezza sia stata ristabilita.
In altre parole, una patch chiude una porta, senza verificare che le finestre siano state messe in sicurezza. E questo i criminali informatici lo sanno.