Attacco massiccio ai dispositivi iOS e macOS

Apr 19, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Scenario, Vulnerabilità 0

I pirati prendono di mira Mac e iPhone. La favola della "sicurezza intrinseca" di computer e dispositivi mobili di Apple traballa sempre di più.

La speranza è che le notizie di cronaca possano funzionare come un campanello di allarme che spezzi l'incantesimo di cui sono troppo spesso vittima gli utenti Apple, ancora convinti in gran parte che i loro dispositivi non abbiano bisogno di antivirus perché "immuni" a malware e attacchi informatici.

E proprio questa curiosa "allergia" a utilizzare software di protezione potrebbe essere alla base degli attacchi che hanno interessato gli utenti macOS e iOS in questi ultimi mesi.

Partiamo dalla campagna che ha preso di mira **iPhone e iPad**, attraverso una falla di sicurezza all'interno della **versione iOS di Chrome**. A sfruttarla è stato il gruppo **eGobbler**, dirottando la navigazione delle vittime su pagine o pop-up che contengono malware.

L'attacco, che secondo **Confiant** (qui il report completo) avrebbe colpito almeno 500 milioni di utenti, utilizza un JavaScript per sfuggire alla sandbox del browser di Google.

I guai derivanti dal gruppo eGobbler, però, è solo l’ultimo i una lunga serie per gli utenti Apple. In questi giorni il rapporto tra l’azienda di Cupertino e la cyber-security è finito anche sotto la lente d’ingrandimento di **Check Point**, che ha pubblicato su Internet una sorta di enciclopedia dei malware per macOS.

L’azienda israeliana, in un comunicato stampa, focalizza l’attenzione soprattutto su due episodi. Il primo riguarda CreativeUpdate, un cryptominer individuato nel febbraio 2018 e che è stato diffuso attraverso il sito MacUpdate.

Il vero “pezzo forte”, però, è **Flashback**, un trojan comparso per la prima volta nel 2011 e che **ha colpito più di 500.000 Mac**.

Flashback utilizza una serie di tecniche estremamente sofisticate per nascondere la sua presenza e rendere più difficile la rilevazione. Tra queste, un complicatissimo sistema che subordina l’esecuzione del malware stesso all’identificativo della macchina su cui è stato installato.

In questo modo il codice non verrà eseguito correttamente su un’altra macchina eccetto quella su cui è stato iniettato in precedenza. Per ottenere questo risultato, **Flashback crittografa la struttura dei suo i dati usando l’UUID della macchina attraverso un sistema di cifratura RC4**.

Una nota curiosa: il malware utilizza **Twitter** come vettore per inviare i comandi tra server Command & Control e computer infettato.

Gli esempi citati, però, sono solo alcuni dei più clamorosi in un casistica molto più ampia che dimostra, ancora una volta, come la piattaforma non possa essere considerata un fattore di riduzione del rischio di attacchi informatici.

Quando riusciremo a spiegarlo ai “talebani del Mac”, forse, avremo fatto un passo avanti nel garantire un maggior livello di protezione per tutti.

Please follow and like us:

I bot pirata rappresentano il 20% del traffico su Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/04/19/attacco-massiccio-ai-dispositivi-ios-e-macos/