Come ti installo il malware sfruttando una falla del mouse

Set 30, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Nuova vulnerabilità nel software di gestione dei dispositivi Kensington. Basta attirare la vittima su un sito Web per installare un malware sul PC.

Dobbiamo preoccuparci di eventuali vulnerabilità del nostro mouse? La risposta è sì. A dimostrarlo, una nuova vulnerabilità nelle periferiche prodotte da **Kensington** che permetterebbe a un pirata informatico di avviare l'esecuzione di codice in remoto sul computer sfruttando una falla del software di gestione di un mouse.

Il programma si chiama **KensigntonWorks** e ha il compito di gestire il complicato sistema di controllo dei mouse a marchio Kensington.

A rendere pubblica la vulnerabilità è stato **Robert Heaton**, che in passato aveva già individuato altre falle di sicurezza nel software di Kensington.

Secondo il ricercatore, la vulnerabilità richiederebbe, per essere sfruttata, soltanto di indurre la vittima a visitare un sito Web sotto il controllo di un pirata informatico e fare in modo che vi rimanga collegato per qualche minuto. Nulla di troppo difficile, quindi.

Ma come funziona il bug? Tutto è collegato all'architettura utilizzata per la gestione delle impostazioni del mouse, che in realtà sfruttano una funzionalità **Web Server** sulla macchina dell'utente.

Una soluzione che Heaton definisce "una pessima idea" e che affonderebbe le sue radici nella volontà degli sviluppatori di utilizzare **Electron**, una piattaforma che consente di creare applicazioni desktop utilizzando **HTML** e **JavaScript**.

Nel suo report, Heaton spiega che questa scelta consentirebbe a un pirata informatico di avviare un collegamento con il computer della vittima e aprire un reverse shell che consentirebbe di eseguire qualsiasi comando sul PC.

Insomma: il risultato sarebbe un margine di azione tale da consentire di eseguire codice malevolo sul computer del malcapitato e, di fatto, installarvi un malware.

L'elemento più preoccupante è che il produttore non avrebbe risposto in alcun modo alle segnalazioni di Heaton e, di conseguenza, tutti gli utenti che usano KensingtonWorks sarebbero vulnerabili a questa forma di attacco, che ora è

pubblica.

Condividi l’articolo

I pirati di REvil cercano soci e mettono sul piatto 1 milione di dollari

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/30/come-ti-installo-il-malware-sfruttando-una-falla-del-mouse/?utm_source=rss&utm_medium=rss&utm_campaign=come-ti-installo-il-malware-sfruttando-una-falla-del-mouse