

Cyber sicurezza: hacker usano aggiornamento Asus per infettare pc

Data: Invalid Date | Autore: Redazione



ROMA, 25 MARZO - Per almeno cinque mesi, da giugno a novembre del 2018, la società tecnologica Asus ha rilasciato a sua insaputa una backdoor - codice malevolo che consente l'accesso dall'esterno a un attaccante - nei computer di migliaia di clienti, attraverso il sistema di aggiornamento automatico dei propri prodotti. La scoperta è stata fatta dai ricercatori Kaspersky, che hanno individuato due server di Asus ai quali probabilmente gli hacker hanno avuto accesso per sfruttare il canale ufficiale e diffondere l'attacco. Il veicolo dell'attacco è il Software Live Update di Asus, un programma preinstallato nei dispositivi prodotti dall'azienda taiwanese, cui è affidato il compito di tenere aggiornati i computer. Una volta ottenuto l'accesso a due server che contengono l'Asus Live Update software, gli hacker hanno sostituito la versione ufficiale del programma con una contenente i codici necessari all'attacco.

La diffusione di questo software è avvenuta indisturbata per mesi in quanto veniva distribuito tramite certificati ufficiali dell'azienda, e quindi era considerato "affidabile" dai sistemi di controllo e dai software antivirus. Questo tipo di attacco è chiamato "supply chain attack", o attacco di filiera, in quanto agisce a monte dell'utente in una delle fasi di produzione dei dispositivi o dei server. Secondo le stime di Kaspersky, oltre un milione di dispositivi con installato un sistema operativo Windows hanno ricevuto l'aggiornamento.

Articolo scaricato da www.infooggi.it

<https://www.infooggi.it/articolo/cybersicurezza-hacker-usano-aggiornamento-asus-infettare-pc/112740>