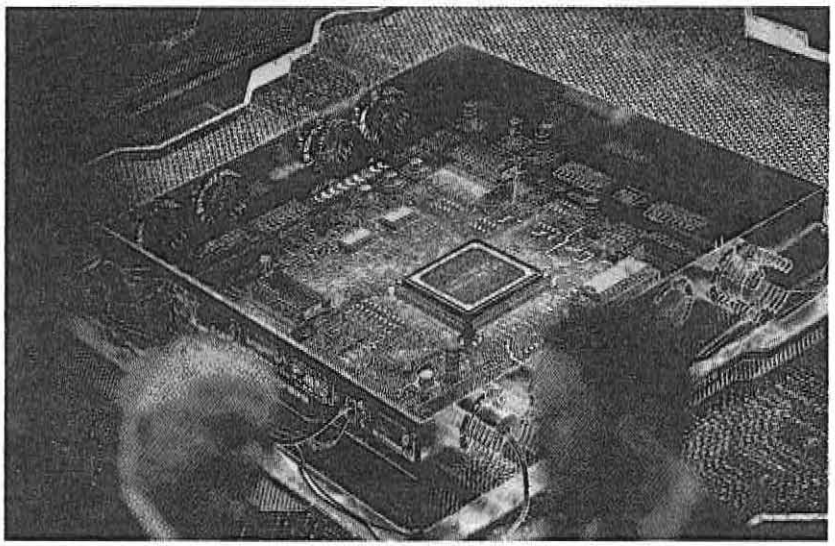
Falle nella sicurezza dei processori A rischio computer e smartphone

I pericoli maggiori arrivano dai browser. Google e Microsoft corrono ai ripari

il caso

CAROLA FREDIANI



1995
Primo bug
Il baco Meltdown è presente sui chip Intel dal 1995

23
gennaio
Chrome, browser di Google, conterrà un importante aggiornamento a partire dal 23 gennaio

Due grosse falle di sicurezza sono rimaste per anni nascoste nel modo in cui sono progettati i processori della maggior parte dei computer. Due vulnerabilità diffuse su un numero enorme e non facilmente quantificabile di pc, smartphone e server, che potenzialmente permettono a un attaccante di accedere a password o altri contenuti sensibili conservati nella memoria di sistema del dispositivo. Il 2018 è iniziato così, coi ricercatori di sicurezza tirati giù dal letto per cercare di mettere una pezza su una delle crisi informatiche più ampie degli ultimi tempi. In realtà le aziende interessate ci stavano lavorando da mesi in gran segreto, dopo le prime segnalazioni ricevute. Ma la notizia è trapelata prima del tempo: di qui la corsa degli ultimi giorni.

Così, dopo anni a parlare di svariate vulnerabilità a livello software, l'hardware si è preso la sua rivincita, mostrando come una falla a livello di progettazione dei processori possa diventare una voragine. Perché i sistemi vulnerabili sono innumerevoli. Perché queste falle sono lì latenti da anni. Perché l'hardware complica tutto. Per dirla con le indicazioni di uno degli organi di risposta alle emergenze informatiche negli Usa, il Cert del Software Engineering Institute, il vero rimedio è uno solo: la sostituzione dei processori. Verdetto brutale, anche contestato, ma per dire che la situazione è complessa. Difficilmente vedremo un richiamo di milioni di computer da parte dei produttori. Che anzi fino a ora nicchiano e minimizzano. Mentre chi produce software e sistemi operativi sta cercando di sfornare aggiornamenti in grado di chiudere o aggirare alcuni di questi problemi. Ma andiamo con ordine. La prima vulnerabilità, battezzata Meltdown da Google, dalla società Cyberus e dall'Università di Graz, è presente su gran parte dei chip Intel a partire dal 1995. La seconda, definita Spectre (trovata da Google e vari ricercatori universitari), su quasi tutti i processori Intel, Amd, Amr, e in generale su quasi ogni moderno processore degli ultimi anni. La dimensione del problema è enorme, ma c'è almeno un dato positivo: le falle più sfruttabili (Meltdown) si possono chiudere con aggiornamenti software; mentre quelle che non si risolvono a breve (Spectre) non sono così facili da usare.

Il bug
Una falla di sicurezza mette virtualmente a rischio tutti i computer, gli smartphone e i tablet in circolazione, insieme ad altri prodotti come smart tv, console per videogiochi e auto connesse

Insomma, gli attacchi sono seri, ma come scrive il ricercatore Martijn Grooten, il loro impatto futuro è difficile da prevedere. Perché sicuramente nelle prossime settimane ci sarà chi troverà modi nuovi per sfruttare queste vulnerabilità. E tuttavia, leggere pezzi arbitrari di memoria, come permesso da queste falle, non si traduce così automaticamente in un'arma; soprattutto è difficile farlo su larga scala. A rischio per ora sembrano essere soprattutto le infrastrutture che offrono servizi cloud.

Per gli utenti normali, l'attacco più preoccupante potrebbe avvenire tramite browser. La fondazione Mozilla ha infatti confermato che Meltdown e Spectre possono essere sfruttate attraverso alcune righe di codice (JavaScript) inserite in un sito web. Per cui basta che un utente col computer vulnerabile visiti quelle pagine ed ecco che un attaccante potrebbe estrarre informazioni riservate che siano elaborate in quel momento dal suo pc. Per questo chi sviluppa browser è corso subito ai ripari. Mozilla ha mitigato l'attacco in Firefox, così come Microsoft con Edge e Internet Explorer 11. Chrome, il browser di Google, conterrà un importante aggiornamento a partire dal 23 gennaio. Poi ci sono i sistemi operativi: Microsoft ha già una «pezza» per Windows 10, altre versioni saranno aggiornate il 9 gennaio. MacOS di Apple dovrebbe avere avuto già alcuni aggiornamenti. Le distribuzioni Linux stanno correndo ai ripari. Agli utenti dunque per ora non resta che aggiornare.