Monitoraggio continuo per combattere il cryptojacking

Author : Redazione

Date : 24 Maggio 2019

È la nuova tendenza nel settore della pirateria informatica e sembra essere diventato lo strumento preferito che i cyber-criminali utilizzano per monetizzare i loro attacchi. Stiamo parlando del **cryptojacking**, la tecnica che permette di sfruttare la potenza di calcolo dei dispositivi infettati per generare cripto-valute che finiscono nelle tasche dei pirati del web.

Gli attacchi che sfruttano il cryptojacking utilizzano due strategie: la prima sfrutta l'inserimento di **JavaScript all'interno di siti Internet** che forzano il browser dei visitatori a sfruttare la CPU del computer o dello smartphone. La seconda fa leva su veri e propri malware, che installano un **miner** (un software dedicato alla generazione di cripto-valuta – ndr) sul sistema della macchina compromessa. Questa seconda strategia, dal punto di vista dei cyber-criminali, è quella più redditizia. I pirati infatti possono sfruttare tutta la potenza del computer, senza rimanere vincolati ai limiti di un processo eseguito all'interno del browser.

Ma quali sono le conseguenze per chi rimane vittima dell'attacco? Oltre ai (soliti) rischi collegati alla violazione dei sistemi, che può portare al furto di dati e alla compromissione di sistemi vitali per l'azienda, il danno più rilevante provocato dai miner è legato all'erosione delle prestazioni. I software di questo tipo, infatti, impegnano il processore dirottandone la potenza di calcolo a scapito delle normali funzionalità. **Risultato: i computer infetti possono subire notevoli rallentamenti, crash di sistema e malfunzionamenti**. In casi estremi, il sovraccarico potrebbe tradursi in un danno fisico della macchina.

Gli attacchi di cryptojacking, inoltre, pongono problemi ulteriori. Trattandosi di programmi che non rientrano "formalmente" nella categoria dei malware, i miner rischiano infatti di sfuggire ai controlli dei normali software di sicurezza, basati sull'analisi del codice e sul sistema delle signature. L'unico indizio di un'attività simile è infatti **un abnorme carico di lavoro riversato sulla CPU**, che un normale utente può notare soltanto andando a controllare il sistema di controllo di Gestione Risorse di Windows.

Coprire questa zona grigia è una sfida che i software antivirus di nuova generazione affrontano attraverso un approccio innovativo, come quello adottato da **Panda Adaptive Defense**. La soluzione di **Panda Security** integra infatti un sistema di monitoraggio che analizza e controlla

ogni singolo processo in esecuzione sulla macchina per individuare eventuali anomalie che possono essere indizio di un attacco di cryptojacking.

A tal proposito, Lara Del Pin, country manager di Panda Security per Italia e Svizzera, afferma che "*Il fenomeno del cryptojacking è in rapida diffusione e sta superando quello del ransomware poiché molto meno rischioso, il threat è più silente, non costa nulla e solo l'attaccante ci guadagna a discapito dell'azienda*".

Per ulteriori informazioni https://www.pandasecurity.com/it/business/adaptive-defense/