La rivincita sui criminali informatici

Scopri di più

Il 60% dei CIO ritiene che gli hacker stiano avendo la meglio nella lotta al cybercrimine[1]. Quindi, in che modo è possibile sviluppare una strategia di sicurezza vincente?

Proprio quando credi di aver rafforzato la tua sicurezza tamponando le eventuali falle che mettono a repentaglio la tua rete, ecco un nuovo attacco informatico: più sofisticato e più persistente dell'ultimo, e pronto a compromettere il tuo business. Sembra non vi sia sosta nell'evoluzione di questi attacchi: ecco perché il 68% dei CIO ritiene che i propri strumenti per la sicurezza non siano adatti a contrastare la minaccia[1].

Ne è prova il recente attacco del 2018, che ha avuto come obiettivo il BIOS di diverse organizzazioni di alto profilo, attaccato con malware ora noti come LoJax[2]. È da tempo che gli attacchi al BIOS generano preoccupazione, in quanto possono essere virtualmente impossibili da individuare, sono estremamente difficili da rimuovere e possono garantire agli hacker un controllo quasi totale dei PC infetti.

E, sebbene questo tipo di attacco sia sempre esistito, non aveva mai rappresentato una minaccia reale per le aziende. Fino ad ora.

Se c'è qualcosa che LoJax mette in evidenza, è sicuramente che non appena si accende il PC, il sistema è vulnerabile a un attacco. I software antivirus e altre soluzioni software di terzi non sono sufficienti a proteggere le reti, soprattutto perché non sono in grado di rilevare alterazioni nel BIOS. Quindi, invece di seguire il 79% delle aziende che si affidano soltanto[3] a software antivirus, è necessario sviluppare una strategia di sicurezza alternativa. Come? Attraverso soluzioni di sicurezza multilivello integrate direttamente nell'hardware.

Noi di HP sappiamo che la scelta dei PC è anche una decisione sulla sicurezza. Ecco perché abbiamo progettato la gamma HP Elite che mette la sicurezza al primo posto, e include PC, workstation e dispositivi POS per il retail. Ad esempio, HP EliteBook x360, con processori opzionali Intel® Core™ i7 di ottava generazione, dispone di funzioni di sicurezza basate sull'hardware stesso, in grado di fornire una difesa multilivello e completa per il tuo business.

I dipendenti che lavorano fuori ufficio e in viaggio sono un bersaglio privilegiato per gli hacker visivi

Funzioni di sicurezza innovative, come HP Sure View Gen2[4]: uno schermo per la privacy integrato e opzionale che ti protegge istantaneamente dall'hacking visivo. Oppure HP Sure Click[5], che protegge l'utente da link ingannevoli e file infetti durante la navigazione sul web. È il PC stesso infatti a creare una sessione di navigazione isolata, impedendo la diffusione del malware da una scheda infetta all'altra.

Oppure, se un attacco come LoJax colpisce l'azienda, è possibile continuare a lavorare in sicurezza e serenamente sapendo che il proprio PC dispone di una funzione di sicurezza avanzata. Una innovazione assoluta nel campo delle tecnologie di riparazione automatica a livello di BIOS, HP Sure Start Gen4[6] rileva automaticamente un attacco malware, anche se inedito , e ripristina il BIOS.

Tuttavia, rafforzare l'attività con questi dispositivi all'avanguardia potrebbe non essere una soluzione immediatamente accessibile. In questi casi, sono utili soluzioni come HP Device as a Service (DaaS)[7]. HP DaaS semplifica la fornitura ai dipendenti dell'hardware, gli accessori e i servizi per il ciclo di vita più adatti, il tutto con un approccio flessibile che soddisfa le esigenze di ogni azienda in tema di sicurezza.

Per scoprire in che modo rendere più sicura la tua attività e per conoscere alcune misure da adottare per proteggerla dagli attacchi informatici, leggi il nostro Manuale operativo di sicurezza informatica.

Fonti:

[1] https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
[2] ricerca ESET: "LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group", ottobre 2018, https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group
[3] Statista Survey ID 622857, "Small and medium sized enterprises in the U.S.", Statista, ottobre 2016
[4] Lo schermo per la privacy HP Sure View integrato è una caratteristica opzionale che deve essere configurata al momento dell'acquisto.
[5] HP Sure Click è disponibile sulla maggior parte dei PC HP e supporta Microsoft® Internet Explorer, Google Chrome e Chromium™. Gli allegati supportati includono i file Microsoft Office (Word, Excel, PowerPoint) e PDF in modalità di sola lettura, se Microsoft Office o Adobe Acrobat ono installati.
[6] HP Sure Start Gen4 è disponibile sui prodotti HP Elite e HP Pro 600 dotati di processori Intel® o AMD di ottava generazione.
[7] I piani HP DaaS e/o i componenti inclusi possono variare per regione o in base al partner di servizio HP DaaS autorizzato. Per informazioni specifiche sulla vostra zona, contattate il rappresentante HP locale o un partner DaaS autorizzato. I servizi HP sono regolati dai termini e dalle condizioni di servizio applicabili di HP, forniti o indicati al cliente al momento dell'acquisto. Il cliente può disporre di ulteriori diritti legali in base alle leggi vigenti nel Paese in cui risiede e tali diritti non sono in alcun modo influenzati dai termini e dalle condizioni del servizio o dalla garanzia limitata HP fornita con il prodotto HP acquistato.

4AA7-5353ITIT, aprile 2019