CYBERSECURITY

Hacker, perché bisogna temere gli attacchi "silenti"

20 Febbraio 2023 11:22

di Chiara Rossi

Gli effetti rilevati all'indomani dell'attacco hacker sulla vulnerabilità VMware ESX sono esigui, tuttavia "non è da escludere la possibilità che l'evento si possa manifestare nella sua interessa in una fase successiva" secondo il ceo di NetGroup, Giuseppe Mocerino

Solo una ventina di server le "vittime" in Italia del "massiccio attacco" hacker avvisato dall'Agenzia nazionale per la cybersicurezza (Acn) nazionale a inizio mese.

Il 5 febbraio l'Acn ha reso noto che "Il Computer Security Incident Response Team Italia (Csirt-IT) dell'Acn ha rilevato un massiccio attacco" hacker "tramite ransomware già in circolazione che prende di mira i server VMware ESXi", aggiungendo che l'attacco era in corso in tutto il mondo e riguardava "qualche migliaio di server compromessi dai paesi europei come Francia – paese più colpito – Finlandia e Italia, fino al Nord America, in Canada e negli Stati Uniti".

Gli esperti dell'agenzia hanno definito il rischio "alto-arancione". Ma che si trattasse di una cosa seria lo ha confermato il vertice convocato con urgenza da palazzo Chigi con il Sottosegretario con la delega alla Cybersecurity Alfredo Mantovano, il direttore dell'Acn Roberto Baldoni e la direttrice del Dis Elisabetta Belloni, per fare un primo bilancio dei danni provocati e mettere in campo le adeguate contromisure.

Eppure numerosi esperti italiani di sicurezza informatica hanno subito ridimensionato la portata dell'attacco, prima ancora di sapere il numero esatto di server effettivamente colpiti.

"Sicuramente gli effetti che sono emersi a valle di questo attacco – almeno quelli noti – sono stati abbastanza irrilevanti. Però si è trattato di un attacco silente che potrebbe comportare altri tipi di conseguenze". È quanto sottolinea a *Startmag* Giuseppe Mocerino, ingegnere, presidente di Netgroup, società che opera nel settore ICT, a proposito degli attacchi informatici di inizio mese.

Tutti i dettagli.

RISCHIO BACKDOOR NELLA FALLA SFRUTTATA DALL'ATTACCO HACKER

"La piattaforma che ha subito l'attacco VMware ESXi è una piattaforma utilizzata da migliaia di imprese italiane e facendo un calcolo tra il numero di installazioni della piattaforma e i segnali di problemi di vulnerabilità segnalate, c'è qualcosa che potrebbe indurre a pensare che non è esclusa la possibilità di aver utilizzato delle backdoor silenti, cioè delle porti d'ingresso silenziose che potrebbero essere attivate in una fase successiva", spiega Mocerino.

"Gli attacchi silenti – aggiunge – sono quelli che destano maggior preoccupazione, dal momento che potrebbero essere attivati e innescati in un secondo momento. Ancora, le backdoor sono delle sentinelle silenziose che ascoltano, vanno a investigare i dati presenti sulle piattaforme".

Secondo il presidente di Netgroup, "gli effetti rilevati all'indomani dell'attacco su questa vulnerabilità sono un numero esiguo, tuttavia non è da escludere la possibilità che l'evento si possa manifestare nella sua interessa in una fase successiva".

GIOCA IL FATTORE UMANO

Come spiegato dallo stesso Csirt, VMware (produttrice americana dell'omonimo sistema informatico preso di mira) aveva già individuato e sanato la vulnerabilità nel febbraio 2021. Tuttavia, non tutti coloro che usano i sistemi attualmente interessati l'hanno risolta. I server presi di mira, se privi delle patch, cioè delle "correzioni" adeguate, possono aprire le porte agli hacker impegnati a sfruttarla.

Ecco dunque che entra in gioco il fattore umano oltre quello tecnologico.

Osserva Mocerino: "Gioca il fattore umano nella protezione di dati e infrastrutture. Innanzitutto, ha un ruolo fondamentale il patching, la messa in sicurezza di falle individuate sulle piattaforme informatiche (Qui l'approfondimento su Cybersecurity, ecco chi investe poco in sicurezza. Report *Startmag*-Icinn). Ne vengono rilasciate migliaia al giorno. Quindi da un lato c'è un'attività automatica con software che distribuiscono queste patch, ma dove non c'è l'automatismo entra in gioco l'intervento umano che deve provvedere all'aggiornamento. Sicuramente non è un problema tecnologico, ma legato al fattore umano che deve avere sensibilità ed esperienza per prevenire queste attività".

EVOLUZIONE DELLE BANDE DI CYBER-CRIMINALI

Inoltre, negli ultimi mesi c'è stata un'evoluzione delle bande di cyber-criminali.

"Fino a un anno fa erano organizzazioni chiuse, composte da cyber-esperti, ma in un numero ben identificato, soprattutto i più pericolosi. Dalla guerra in Ucraina in poi, si è verificato un fenomeno: sul dark web vengono resi disponibili, in maniera aperta, tutti gli strumenti per poter avviare un'attività di hacking. Quindi questo ha consentito il proliferare, in pochissimo tempi, di tanti piccoli gruppetti che hanno accesso ai tool per violare i sistemi e, in autogestione, si organizzano in una maniera più o meno strutturata per iniziare una serie di attacchi (dal ransomware al ddos)", spiega il ceo di Netgroup.

Aumenta così di molto il perimetro degli attacchi cyber e, allo stesso tempo, è molto difficile andare a effettuare un'attività di controllo, secondo Mocerino.

COSA SI PUÒ FARE

Dunque "L'attività di controllo passa attraverso un'attività predittiva e di prevenzione. Occorre avere all'interno delle organizzazioni pubbliche e private un expertise dedicato solo al monitoraggio del livello di sicurezza di sistemi, che va misurato costantemente. Va sensibilizzata l'organizzazione pubblica e privata affinché si doti, non tanto di tecnologia, ma di know-how interno che devono applicare la buona prassi di mantenimento di un buon livello di sicurezza", conclude il presidente di Netgroup.

Fondamentale si rileverà quindi il monitoraggio costante del livello di sicurezza dei sistemi.