“Never trust your victim”: il Laboratorio Nazionale di Cybersecurity ha scoperto una vulnerabilità che avrebbe potuto esporre gli analisti di sicurezza informatica

Cara collega, caro collega,
i ricercatori del Laboratorio Nazionale di Cybersecurity del Cini (Consorzio interuniversitario nazionale per l’informatica) hanno scoperto e segnalato una **vulnerabilità** in Metasploit Pro, popolare strumento utilizzato da analisti di sicurezza informatica e hacker in tutto il mondo, che avrebbe potuto esporre chi lo utilizza a un attacco, a partire proprio dal dispositivo sottoposto ad analisi.

Sviluppato dall’azienda statunitense Rapid7, Metasploit Pro fornisce a ricercatori ed esperti di sicurezza informatica diversi strumenti di analisi ed esecuzione di attacchi, particolarmente utili nelle operazioni di penetration testing. Tra queste anche la funzione di scansione delle vulnerabilità, che esegue una lettura automatica dell’infrastruttura sottoposta ad analisi.

I ricercatori **Gabriele Costa** (Scuola IMT Alti Studi Lucca), **Andrea Valenza** e **Alessandro Armando** (Università di Genova) hanno scoperto che era possibile far sì che Metasploit Pro rilevasse ed eseguisse un payload malevolo in Javascript. Dal momento che Metasploit Pro si avvale di un backend e del normale browser del computer dell’analista, era possibile fare in modo che, **durante la scansione**, il server analizzato prendesse il controllo del browser, attraverso il quale è possibile infine eseguire dei comandi sullo stesso sistema operativo dell’analista. Dal momento che Metasploit Pro richiede i privilegi di root per funzionare (e quindi ha le autorizzazioni per eseguire qualsiasi comando all’interno del sistema operativo), l’attaccante avrebbe potuto **prendere il completo controllo della macchina dell’analista**.

In parole povere, un attaccante in controllo del server sottoposto ad analisi avrebbe potuto sfruttare questa vulnerabilità per attaccare lo stesso analista che sta eseguendo una scansione della macchina alla ricerca di intrusioni informatiche, eventualmente sabotandone l’attività e acquisendo un vantaggio rispetto alle sue vittime.

Alle vulnerabilità individuate sono stati assegnati i codici Cve (Common Vulnerabilities and Exposures, dizionario delle vulnerabilità pubblicamente note) CVE-2020-7354 e CVE-2020-7355. Come da consuetudine, l’azienda è stata prontamente messa al corrente del problema, al quale ha immediatamente posto rimedio.

“Generalmente un predatore non si aspetta di poter essere, a sua volta, la preda” commenta **Gabriele Costa**, ricercatore presso la Scuola IMT Alti Studi Lucca e tra gli autori della scoperta. *“Quello è il momento in cui siamo più vulnerabili ed è proprio la fase in cui abbiamo individuato la vulnerabilità. Non si tratta di un tipo di attacco tecnicamente complesso, ma è proprio per questo che l’impatto avrebbe potuto essere drammatico. Fortunatamente gli esperti di Rapid7 hanno subito compreso il rischio e si sono attivati per mettere in sicurezza Metasploit Pro in tempi brevissimi”*.

“In Rapid7 siamo consapevoli che non esiste un attacco tanto intrigante quanto quelli che prendono di mira i software usati per la sicurezza, e ‘hackerare gli hacker’ è la ricompensa stessa, quando si parla di difesa attiva”, commenta **Tod Beardsley**, direttore del dipartimento di ricerca di Rapid7. *“Siamo sempre alla ricerca di vulnerabilità nei nostri prodotti per la sicurezza, quindi apprezziamo il lavoro svolto dal Laboratorio Nazionale di Cybersecurity dell’Italia e l’opportunità che abbiamo avuto di rendere il nostro prodotto più sicuro”*.

Che cos’è il Laboratorio Nazionale di Cybersecurity - CINI

Il Laboratorio Nazionale di Cybersecurity del CINI coordina attività di ricerca, sviluppo e formazione sui temi della sicurezza informatica a livello nazionale e internazionale per aiutare il sistema paese a essere più resiliente alle minacce cibernetiche. Il Laboratorio si impegna quindi a migliorare le misure di protezione della pubblica amministrazione e delle imprese da attacchi informatici supportando anche i processi di definizione degli standard e dei framework metodologici a livello nazionale. https://cybersecnatlab.it/

Raffaele Angius
Responsabile della comunicazione, Laboratorio Nazionale di Cybersecurity
+39 320 0869746
comunicazione.cybersecurity@consorzio-cini.it