Attacco alle app Web per il sequenziamento del DNA

Giu 17, 2019 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I pirati sfruttano una falla nelle applicazioni. L'origine dell'attacco in Iran, ma i ricercatori hanno dubbi sugli obiettivi e identità degli attaccanti.

Un attacco coordinato che sta prendendo di mira da giorni alcune **applicazioni Web per il sequenziamento del DNA**. A denunciarlo è **Ankit Anubhav**, che attraverso il suo profilo Twitter ha segnalato l'inizio degli attacchi lo scorso 12 giugno.

I pirati informatici si stanno concentrando su **dnaLIMS**, un'applicazione utilizzata da università e organizzazioni di vario genere per contribuire all'analisi e il sequenziamento del DNA.

Gli attacchi, spiega Anubhav, sfruttano una vulnerabilità (CVE-2017-6526) scoperta nel 2017, che lo sviluppatore dell'applicazione non ha però corretto.

La falla di sicurezza consentirebbe, nel dettaglio, di impiantare delle shell che consentono di controllare in remoto il Web Server su cui gira dnaLIMS.

Difficile, però, capire quale sia il reale obiettivo dei pirati informatici. **Secondo i ricercatori, l'origine degli attacchi sarebbe in Iran, un indizio che farebbe pensare immediatamente a un'azione collegata al governo di Teheran**.

Oltre alla "normale" cautela nell'attribuzione degli attacchi informatici, però, in questo caso a suggerire di non saltare a conclusioni affrettate contribuiscono anche altri elementi.

Per esempio il fatto che non sia ancora chiaro quali siano i reali obiettivi dei pirati informatici. **Se il primo pensiero è quello che possano puntare a rubare i dati processati sui server, non è escluso che abbiano come scopo "solo" quello di poter infettare le macchine per altri obiettivi, come quello di reclutare i dispositivi in una botnet o installare miner per la generazione di cripto-valuta**.

Tanto più che gli indirizzi IP individuati dai ricercatori come origine dell'attacco sono stati utilizzati in passato per operazioni decisamente più "prosaiche", che hanno preso di mira dei router **Zyxel** e installazioni di **Apache Struts** sfruttando bug piuttosto conosciuti.

Insomma: l'impressione è che più che a un gruppo di hacker al soldo del governo iraniano, ci si trovi di fronte a quelli che gli esperti di sicurezza chiamano **script kiddie**, cioè

principianti che usano codice che sfrutta vulnerabilità conosciute e che, in realtà, non hanno livelli di professionalità degni di nota.

Il problema, però, rimane e c'è da chiedersi se gli sviluppatori di dnaLIMS non si decideranno infine a distribuire una patch per correggere la vulnerabilità sfruttata dai pirati.

Condividi l'articolo

Triplicato l'interesse dei bambini per i siti di ecommerce

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/06/17/attacco-alle-app-web-per-il-sequenziamento-del-dna/