Criptovalute, nel 2017 oltre 170 milioni di attacchi di web mining

Il fine settimana appena passato ha visto un nuovo boom di siti web sfruttati in maniera criminale e all'insaputa dei proprietari per far estrarre criptovalute in maniera illecita tramite azioni di ***web mining***. Stavolta, però, sono stati messi a lavorare i siti web e le piattaforme non di singoli cittadini, ma delle amministrazioni pubbliche.

In totale oltre **4000 siti**, tra cui le **piattaforme governative del Regno Unito e della Corte federale degli Stati Uniti**. Tutti questi siti avevano in comune l'uso del medesimo plugin *BrowseAloud* di TextHelp (già rimosso dall'azienda), un "cavallo di Troia" che legge le pagine web per le persone ipovedenti o con problemi di lettura di varia natura, tra cui la dislessia.

Il *miner* in questione è il **Monero di CoinHive** e funziona come tutti gli altri: su innumerevoli siti web vengono integrati *script* di *mining* che usano le risorse del computer del visitatore (quasi sempre all'oscuro di tutto) per minare criptovalute.

Riguardo a quest'ultima ondata di *web mining* criminale, **Anton Ivanov**, Lead malware expert di Kaspersky Lab, ha commentato: "*L'attacco riportato prevede un approccio conosciuto come web mining, che non comporta l'installazione di alcun codice nocivo sul dispositivo della vittima, mentre le attività di mining vengono condotte attraverso un codice speciale situato in una pagina web infetta. Secondo i nostri dati, l'infezione ha avuto luogo l'11 febbraio, tra le ore 11:20 GMT/UTC e le 16:10 GMT/UTC. Durante questo arco temporale, i nostri sistemi*

hanno registrato tentativi di caricare la versione infettata dello script di plug-in su almeno 450 siti”.

Solo durante **lo scorso anno sono stati bloccati oltre 170 milioni di attacchi di web mining** e **gli utenti di internet coinvolti sono stati circa 7,3 milioni** in tutto il mondo: “*Il web miner più usato è stato CoinHive, che è stato impiegato anche per l’attacco riportato. Il malware è stato iniettato nei siti offrendo una soluzione plug-in ampiamente utilizzata per leggere ad alta voce le pagine web. Solo pochi giorni fa, è stato scoperto un episodio simile che riguarda CoinHive e ha coinvolgo YouTube, con web miner installati nelle pubblicità contestuali*”, ha spiegato il ricercatore.

Il pericolo rappresentato dal *mining* di criptovalute non riguarda la perdita di dati o denaro, “*ma **l’impatto sulla performance del sistema e sul consumo energetico.** Il mining ha infatti un impatto significativo sulle risorse del sistema. Inoltre, venir colpiti da un simile attacco potrebbe comportare per le aziende importanti conseguenze reputazionali*”, ha precisato Ivanov.

Tuttavia, ha suggerito l’informatico, “*va sottolineato che non tutte le attività di web mining sono illegali. In alcuni casi, vengono utilizzate legittimamente per la monetizzazione dei siti web: gli utenti ricevono i contenuti dei siti in cambio dell’accesso alle risorse del proprio computer, utilizzate per il mining*”.

> *Criptovalute, nel 2017 oltre 170 milioni di attacchi di web mining*