Il worm Graboid fa strage di Docker vulnerabili

Ott 17, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Si installa e sfrutta i server per generare cripto-valuta utilizzando un sistema di attivazione casuale che lo rende più difficile da individuare.

L'ennesimo attacco che prende di mira la piattaforma **Docker** questa volta vede come protagonista un worm. Si tratta di **Graboid**, un cryptominer che è stato scoperto dal team **Unit 42** di **Palo Alto Networks**.

Docker è una piattaforma estremamente diffusa, che permette di creare dei "pacchetti" chiamati container al cui interno ci sono applicazioni in grado di girare su cloud come se fossero su una macchina virtuale, ma senza che sia necessaria la presenza di un vero e proprio sistema operativo. **Negli ultimi mesi, però, Docker è diventata il bersaglio preferito dei pirati informatici**.

Nel caso di Graboid, l'attacco prende di mira le installazioni Docker che non hanno protezione, cioè quelle per cui gli amministratori **non hanno predisposto un sistema di autenticazione per il caricamento dei pacchetti**. Stando a quanto raccontano i ricercatori nel report pubblicato sul blog di Palo Alto Network, in circolazione ce ne sarebbero almeno 2.000.

Il container usato dai cyber-criminali contiene due moduli. Il primo è programmato per diffondere il worm individuando nuovi bersagli attraverso le indicazioni che provengono dal server Command and Control. Il secondo contiene invece un miner **xmrig**

che sfrutta la potenza del server compromesso per generare **Monero**, la cripto-valuta preferita dai pirati informatici.

L’attacco avviene in sei passaggi:

1 Il pacchetto **pocosow/centos:7.6.1810** viene installato utilizzando dei comandi in remoto sull’host vulnerabile. Al suo interno è presente uno strumento che permette di comunicare con gli altri host Docker.

2 In seguito viene avviato lo script **/var/sbin/bash**, che scarica quattro script shell (**live.sh**, **worm.sh**, **cleanxmr.sh**, **xmr.sh**) dal server Command and Control (c2) e li esegue uno per uno.

3 Lo script **live.sh** invia al server C2 informazioni sul numero di CPU disponibili sull’host compromesso.

4 L’esecuzione di **worm.sh**, invece, avvia il download di un elenco con oltre 2.000 indirizzi IP. Si tratta degli host Docker vulnerabili all’attacco. Lo script comincia a inviare i comandi in remoto per installare il pacchetto infetto su ogni host indicato nell’elenco.

5 Qui le cose si fanno strane: cleanxmr.sh è infatti

programmato per scegliere casualmente un host dall’elenco e bloccare il miner attivo al suo interno.

6 L’ultimo script (**xmr.sh**) seleziona casualmente un host dall’elenco e installa il container **gakeaws/nginx** che contiene il miner.

Questa strana procedura fa in modo che il funzionamento del modulo di crypto-jacking sia molto particolare. Si attiva per periodi di tempo limitati e lo fa in modo apparentemente casuale. **Dalle simulazioni effettuate dai ricercatori, i miner sono attivi solo per il 65% del tempo per periodi di tempo che in media non superano i 4 minuti**.

Probabilmente la tecnica punta a rendere più difficile l’individuazione del miner, che solitamente viene effettuata attraverso l’analisi dei carichi di lavoro delle CPU. Non solo: visto che l’attività di mining non comincia subito dopo l’installazione, l’analisi dei log non mostra un’immediata corrispondenza tra il download di un pacchetto e l’aumento dell’attività della CPU.

Il loro attacco, però, è decisamente efficace. **Secondo la Unit 42, i pirati hanno a disposizione 1.400 processori e una potenza di calcolo complessiva di circa 900 CPU**. Tradotto in parole povere: stanno intascando un mucchio di soldi.

Condividi l’articolo

I pirati attaccano i programmi fedeltà

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/10/17/il-worm-graboid-fa-strage-di-docker-vulnerabili/