Attacco massiccio a Docker. I pirati usano Shodan per colpire gli host

Mag 31, 2019 Marco Schiaffino Attacchi, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

La campagna punta a distribuire container al cui interno è nascosto un miner per generare cripto-valuta. Colpiti almeno 10.000 server.

Una vera emergenza che avrebbe coinvolto migliaia di host **Docker** e che gli esperti di sicurezza stentano a contenere. L'attacco individuato da **Trend Micro**, che ne ha pubblicato i dettagli in questo report, ha caratteristiche che lo collocano a metà tra una botnet e un worm.

Docker è una piattaforma che permette di creare dei "pacchetti" (container) che contengono applicazioni in grado di girare su cloud come se fossero su una macchina virtuale, ma senza che sia necessaria la presenza di un intero sistema operativo per supportarle. La piattaforma è popolarissima e sfrutta una rete di Hub da cui è possibile scaricare e installare i container.

Nel dettaglio, i cyber-criminali individuati da Trend Micro prendono di mira gli host Docker che hanno API esposte su Internet attraverso la porta 2375 per violarne i sistemi di sicurezza tramite una tecnica di **brute forcing**.

Una volta ottenuto l'accesso, utilizzano uno script (ubu.sh) per caricare l'immagine infetta del container. Al suo interno sono presenti alcuni script aggiuntivi utilizzati dai pirati per installare il payload e diffondere ulteriormente i

container infetti.

Per quanto riguarda il payload, si tratta di un classico miner in grado di sfruttare la potenza di calcolo del server per generare cripto-valuta (il solito **Monero**) che viene depositata sui conti dei pirati informatici. La scelta di Monero non è casuale.

Oltre a garantire un livello di anonimato superiore a quello di altre monete virtuali, Monero ha un'altra caratteristica utile ai cyber-criminali: mentre i miner di altre cripto-valute (per esempio Bitcoin) sono ottimizzati per l'uso con i processori grafici che eseguono calcolo parallelo, quelli di Monero offrono le migliori prestazioni con le normali CPU.

La vera "chicca" in questo attacco però riguarda il sistema di diffusione scelto dagli hacker. Il modulo a cui è affidato questo compito utilizza infatti **Shodan** (un motore di ricerca

in grado di individuare i dispositivi collegati a Internet – ndr) per localizzare nuove potenziali vittime e avviare l'attacco.

Gli indirizzi IP degli host vulnerabili vengono inseriti in un file di testo (**iplist.txt**) e poi verificati uno per uno. Se al loro interno viene rilevato un miner già attivo, gli indirizzi vengono cancellati. In caso contrario parte l'attacco. **Insomma: in questo modo i container infetti si diffondono autonomamente**.

I ricercatori di Trend Micro hanno individuato l'attacco quando hanno analizzato un container "comparso" su un loro honeypot (i server usati dalle società di sicurezza come "falsi bersagli" per i malware) che proveniva da un Docker Hub chiamato **zoolu2**.

Sarebbe proprio questo, secondo i ricercatori, il repository all’origine dell’attacco. Ma da quanto va avanti? Dalle loro analisi risulta che le immagini sono state caricate nel mese di maggio, ma nel report sottolineano come i container siano stati più volte aggiornati ed è probabile, di conseguenza, che l’attacco sia iniziato prima.

Ora l’account di zoolu2 è stato disattivato, così come gli account Shodan usati per le ricerche e un altro account Docker (**Pavlov32**) che aveva le stesse caratteristiche di zoolu2. A quanto pare, però, una delle immagini container infette

sarebbe stata già scaricata più di 10.000 volte.

Il suggerimento degli esperti di sicurezza per gli utenti è quello di controllare le impostazioni per verificare che container e API non siano raggiungibili dall'esterno, implementando sistemi di autenticazione per impedire intrusioni come queste.

Condividi l'articolo

Rivoluzione GitHub: ecco gli aggiornamenti automatici per i pacchetti

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/31/attacco-massiccio-a-docker-i-pirati-usano-shodan-per-colpire-gli-host/