Protezione cloud: l’obiettivo è controllare i container

Mag 23, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

Dopo gli attacchi che colpiscono la filiera DevOps gli esperti prendono le contromisure. Trend Micro: “Ecco come proteggiamo le applicazioni cloud”.

Tecnicamente si chiamano attacchi **supply chain**, cioè attacchi che prendono di mira gli sviluppatori per andare a colpire la vittima designata (o più vittime) che utilizza i componenti software infetti.

Con l’esplosione del cloud, questa tecnica di attacco è diventata non solo più popolare tra i pirati informatici, ma anche più insidiosa. Il sistema che utilizza i container per implementare funzionalità attraverso “pacchetti” già pronti offre infatti un formidabile vettore di attacco per i cyber-criminali.

La cronaca recente conferma la tendenza: gli ultimi attacchi a **Docker** (ne abbiamo parlato in questo articolo) e le vulnerabilità scoperte in **Kubernetes** (in questo articolo) ne sono la conferma più evidente.

Non stupisce, quindi, che le società di sicurezza abbiano puntato i riflettori su questo aspetto della sicurezza su cloud, attivando procedure di controllo per garantire l’integrità dei container ed evitare che possano trasformarsi in un fattore di rischio.



Ora sembra che questo aspetto stia vivendo una fase di ulteriore evoluzione. A proporla è **Trend Micro**, che ha annunciato una serie di nuove funzionalità che puntano a trasformare il controllo dei container, fino a oggi eseguito a livello runtime, in un sistema di monitoraggio che copre tutto il ciclo di vita **DevOps**.

Nel dettaglio, spiegano dalle parti di Trend Micro, i nuovi strumenti comprendono un controllo dell'immagine dei container nella pipeline di creazione software, attraverso una scansione pre-registro che permette di individuare in anticipo le vulnerabilità e i malware, consentendo di individuare eventuali minacce future.

Non solo: il sistema **Deep Security** a cui è affidata l'analisi controlla anche password e chiavi private per verificarne la conformità e analizza tutti i movimenti di traffico laterali e orizzontali tra i container e i livelli della piattaforma.

Tutto questo, ci tengono a specificare gli esperti della società di sicurezza con sede a Tokyo, attraverso **un sistema completamente automatizzato**, sfruttando un ambiente che consente di utilizzare qualsiasi command shell per eseguire API.

Insomma, la strada per espandere alla cloud il concetto di “sicurezza come processo” è aperta. Ora aspettiamo di vederne l’impatto in un settore che negli ultimi tempi ha dimostrato di soffrire più degli altri le indesiderate “attenzioni” dei cyber-criminali.

Please follow and like us:



SandboxEscaper colpisce ancora: altro zero-day per Windows

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/23/protezione-cloud-lobiettivo-e-controllare-i-container/