Ti presento Doki: la backdoor per sistemi virtuali su Linux

Lug 31, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il malware colpisce i server Docker e usa una serie di tecniche basate su blockchain per comunicare con i server Command and Control.

Una nuova minaccia, l'ennesima, prende di mira i servizi virtualizzati su piattaforma cloud e il bersaglio sono ancora una volta i server **Docker**, utilizzati dalle aziende per l'implementazione di servizi virtualizzati "autonomi".

Doki, individuato dai ricercatori di **Intezer**, è una backdoor che consente ai pirati informatici di compromettere i server Linux su cui "girano" i container Docker. A differenza di altri malware che in passato hanno preso di mira questo tipo di piattaforma, che si limitavano a installare dei miner per generare criptovaluta, Doki consente ai pirati informatici un campo di azione maggiore.

La backdoor consente infatti di eseguire qualsiasi tipo di codice sulla macchina infetta e apre la possibilità, di conseguenza, che i cyber criminali installino qualsiasi tipo di payload ulteriore.

Come spiegano gli analisti nel report, gli attacchi vengono portati attraverso un sistema di scansione che individua i server Docker con impostazioni "deboli", in particolare a livello di API, che i pirati sfruttano per violare il sistema.

Per individuare i potenziali bersagli e portare l'attacco, gli autori di Doki utilizzano una botnet basata su **ngrok** (un

servizio di reverse proxy – ndr) individuata tempo fa dagli esperti di sicurezza.

Lo schema di attacco prevede, una volta eseguito l'accesso al server, la creazione di nuovi container che i pirati caricano da un repository pubblico. I container in quesitone, infatti, non contengono direttamente il codice malevolo, ma permettono l'esecuzione di **Curl**, che i criminali sfruttano per i loro scopi.

Uno degli elementi più interessanti evidenziati dai ricercatori di Intezer, però, è il fatto che Doki utilizza un particolare sistema di comunicazione con i server Command and Control, che sfrutta la blockhain di **Dogecoin**, una criptovaluta lanciata nel 2014.

Insomma: utilizzando una botnet basata su reverse Proxy, container apparentemente legittimi e un sistema di comunicazione che sfrutta una tecnica di offuscamento innovativa, Doki rappresenta una minaccia estremamente difficile da rilevare.

Non solo: secondo i ricercatori, che hanno eseguito dei test

usando **Virus Total**, al momento solo 24 motori antivirus su 60 sono in grado di individuare il malware.

Il metodo più efficace per bloccarne la diffusione, in ogni caso, è quello di eseguire una corretta configurazione dei server Docker, avendo cura in particolare di non esporre le API a collegamenti esterni.

Condividi l’articolo

SkyArk: uno strumento open per individuare falle in AWS e Azure

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/31/ti-presento-doki-la-backdoor-per-sistemi-virtuali-su-linux/?utm_source=rss&utm_medium=rss&utm_campaign=ti-presento-doki-la-backdoor-per-sistemi-virtuali-su-linux