Raport consolidat eveniment cibernetic

Cryptojacking ce vizează API Docker și Kubernetes

O campanie recentă de cryptojacking exploatează API-urile Docker expuse și neprotejate prin parolă, permițând atacatorilor să inițieze containere malițioase care minează criptomonede utilizând resursele sistemelor compromise.

Informații suplimentare

TIP	**MALWARE**
Versiuni afectate	Instanțe Docker și Kubernetes cu API-uri expuse public și neprotejate corespunzător.
Impact	**Utilizarea Resurselor Sistemului:** Consumul semnificativ al resurselor de calcul ale sistemelor afectate, ceea ce poate duce la degradarea performanței aplicațiilor legitime. **Compromiterea Securității Infrastructurii:** Posibilitatea ca infrastructura compromisă să fie utilizată pentru atacuri suplimentare sau să devină parte a unui botnet controlat de atacatori.
Exploatare	1. Identificarea API-urilor Docker expuse utilizând instrumente de scanare precum **masscan** și **zgrab.** 2. Inițierea unui container Alpine și montarea sistemului de fișiere al gazdei în interiorul containerului. 3. Executarea unui script de inițializare care descarcă și rulează XMRig pentru minerit de criptomonede.
IOA, IOA și TTPs	**IP adresa atac**

	45.9.148.35, 164.68.106.96, 192.155.94.199, 147.75.47.199 **Hash** 82874f856a71a751f0bdb1ce7a3b7bb6, e10e3934d7659e00cc7f47b569af9ff5, 505237e566b9e8f4a83edbe45986bbe0e893c1ca4c5837c97c6c4700cfa0930a **URLs** hxxp://45.9.148.35/aws, hxxp://solscan.live/sh/init.sh , hxxps://solscan.live/bin/xmrig **TTP** ***T1222.002:*** Linux and Mac File and Directory Permissions Modification, ***T1053.003:*** Cron, ***T1021.004:*** SSH Killchain Stage: Initial Exploitation, Privilege Escalation, Execution, Lateral Movement **Malicious scripts** hxxp://solscan.live/sh/xmr.sh.sh, hxxp://solscan.live/sh/setup_xmr.sh, hxxp://solscan.live/incoming/docker.php?dockerT=
Depistarea	❖ **Scanarea Infrastructurii:** Utilizarea instrumentelor de scanare pentru a identifica API-uri Docker expuse și neprotejate. ❖ **Audituri de Securitate:** Efectuarea de audituri regulate pentru a verifica configurările de securitate și a identifica posibile vulnerabilități.
Măsuri de remediere	1. **Protejarea API-urilor Docker:** Asigurarea că API-urile Docker nu sunt expuse public și implementarea autentificării adecvate. 2. **Monitorizarea Activităților Neobișnuite:**Supravegherea utilizării resurselor și detectarea activităților suspecte care ar putea indica prezența unui miner de criptomonede.

	3. **Actualizarea și Patching-ul Sistemelor:** Menținerea la zi a actualizărilor de securitate pentru Docker, Kubernetes și alte componente ale infrastructurii.

Resurse externe

- https://socradar.io/blog-cryptojacking-campaign-targets-docker-and-kubernetes-surge-in-container-based-attacks/
- https://securitylabs.datadoghq.com/articles/threat-actors-leveraging-docker-swarm-kubernetes-mine-cryptocurrency/?utm_source=chatgpt.com