Severity

Medium

Analysis Summary

Docker Engine honeypots were compromised by Ukraine supports, most likely the Ukraine IT Army, in attacks against Belarusian and Russian websites. DOS (denial-of-service) were conducted on Russian websites by compromising exposed Docker Engine API. The first image “abagayev/stop-russia” was downloaded around 100,000 times.

“Container and cloud-based resources are being abused to deploy disruptive tools. The use of compromised infrastructure has far-reaching consequences for organizations who may unwittingly be participating in hostile activity against Russian government, military and civilian targets.” reported Security Researchers. “Docker Engine honeypots were compromised to execute two different Docker images targeting Russian, Belarusian and Lithuanian websites in a denial-of-service (DoS) attack.”

Impact

- Server Outage
- Data Loss
- Website Downtime

Indicators of Compromise

MD5

- 4e44f3f239e0ccdac47ec56c43cab7be

SHA-256

- 3f954dd92c4d0bc682bd8f478eb04331f67cd750e8675fc8c417f962cc0fb31f

SHA-1

- 8af6c0a9ae9a8d6b0b6218ac920d5e173d690e93

Remediation

- Upgrade your operating system.
- Don’t open files and links from unknown sources.
- Install and run anti-virus scans.
- Block indicators in your environments