Mphasis
The Next Applied

# Millions of Docker repos found pushing malware, phishing sites

Date: 01st May 2024 | Severity: High

## Summary

Three large-scale campaigns targeted Docker Hub users, planting millions of repositories that pushed malware and phishing sites since early 2021. Each of these campaigns used different tactics to create and distribute the malicious repositories.

- The “Downloader” and “eBook Phishing” campaigns created fake repositories in batches.
- The “Website SEO” campaign created a few repositories daily and used a single user per repository.
- Typical attacks targeting developers and organizations directly, the attackers in this case tried to leverage Docker Hub’s platform credibility, making it more difficult to identify the phishing and malware installation attempts,” JFrog added.

## Attack Vectors

This campaign operated in two distinct rounds (circa 2021 and 2023), and both rounds used the same malicious payload, a malicious executable that most antivirus engines detect as a generic Trojan,” said JFrog.

- The malware payload it pushed displays an installation dialog that asks the user to download and install the advertised software.
- Download all the malicious binaries from the offer instead and schedule their persistent execution on the now compromised system.

## Indicator of compromise

| INDICATOR TYPE | INDICATORS | | |
|---|---|---|---|
| Domain | • failhostingpolp[.]ru<br>• gts794[.]com<br>• blltly[.]com<br>• ltlly[.]com<br>• byltly[.]com<br>• bytlly[.]com<br>• cinurl[.]com<br>• fancli[.]com<br>• geags[.]com<br>• gohhs[.]com<br>• imgfil[.]com<br>• jinyurl[.]com | • miimms[.]com<br>• picfs[.]com<br>• shoxet[.]com<br>• shurll[.]com<br>• ssurll[.]com<br>• tinourl[.]com<br>• tinurli[.]com<br>• tinurll[.]com<br>• tiurll[.]com<br>• tlniurl[.]com<br>• tweeat[.]com<br>• urlca[.]com | • urlcod[.]com<br>• urlgoal[.]com<br>• urllie[.]com<br>• urllio[.]com<br>• urloso[.]com<br>• urluso[.]com<br>• urluss[.]com<br>• vittuv[.]com<br>• rd[.]lesac[.]ru<br>• soneservice[.]shop |

# Recommendation

- Minimize the use of third-party software and use verifiable ones to avoid introducing malicious software the container environment.
- Scan images in the repository to check for misconfigurations and determine if they contain any vulnerabilities.
- Prevent vulnerability exploitation by using tools such as Clair, which provides static analysis for containers.
- Host containers in a container-focused OS to reduce the attack surface.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- https://www.bleepingcomputer.com/news/security/millions-of-docker-repos-found-pushing-malware-phishing-sites/
- https://thehackernews.com/2024/04/millions-of-malicious-imageless.html
- https://jfrog.com/blog/attacks-on-docker-with-millions-of-malicious-repositories-spread-malware-and-phishing-scams/