Docker breach exposes a significant number of accounts

Reference: Memo [190430-1] Date: 30/04/2019 - Version: 1.0
Keywords: Docker, supply-chain attack
Sources: publicly available information

Key Points

- Docker Hub, an open repository of software containers, announced a breach affecting about 190 000 of its users.
- As the breach affects associated development platforms, it may impact several stages of software development workflows.
- Threat actors adopt supply chain attacks as a method to bypass some of the traditional IT security measures.

Summary

The open repository of prepared software containers Docker Hub has informed its users that on April 25 it suffered a breach resulting in the exposure of information of approximately 190.000 accounts, including items such as usernames and (hashed) passwords, as well as GitHub and Bitbucket access tokens.

A Docker container is a prepared package of software along with all the pieces of code that it will require to operate. It offers the capability to run a piece of software on an otherwise unprepared platform, without being concerned about software dependencies and missing elements. GitHub and Bitbucket are both code repositories that facilitate code management and cooperation between teams. Their access tokens allow developers to automatically transfer newly developed code to Docker Hub for integration with Docker installation images.

Docker is utilised by a significant number of software producers including several software industry giants in order to deliver ready-to-operate solutions. As such, the main Docker distribution point, the Docker Hub has significant importance for the secure delivery of software products. A breach in any step of this service could potentially allow threat actors to engage in supply-chain attacks (thus introducing unwanted functionalities).

According to information provided by Docker on the incident, the number of affected accounts amount to about 5% of the total Docker Hub users. Another significant detail is that images provided by Docker Hub were highly likely not affected themselves due to the extra checks and code signing employed in the workflow. Still, the potential for affecting Docker users is significant as it includes the code development (GitHub/Bitbucket) aspect.

Comments

Supply chain attacks have been prevalent in 2019. So far there have been two well-known cases, linked to each other. The hardware manufacturer Asus had a breach in a server distributing software updates, discovered in January 2019 but highly likely operating in the period between June and November 2018. The malware was delivered to a large number of systems even though the attackers were interested only in a small number of them. The attack was named ShadowHammer (for additional information, please see CERT-EU Memo [190326-1], issued on 26/03/2019).

Additionally, three different videogame companies were found in April 2019 to be distributing their products infected with malware. Even though the incidents are highly likely linked to the ShadowHammer perpetrators, their breach and subsequent introduction of malware in their products was (according to open sources) likely due to bad developer practices.

In all these cases the end software was signed with the legitimate manufacturer digital certificate.

The incidents underline the intention of threat actors to achieve mass infections while bypassing some of the installed IT security systems by leveraging breached trusted third parties. It is therefore a good protection practice for environments with significant IT security requirements to require from suppliers the same rigorous approach to security (via policies and measures) as the actual organisation. Furthermore, based on the Docker Hub incident, organisations should analyse every step of their development process to identify points were they depend on the implementation of security at external partners and take sufficient measures to mitigate possible risks.

As an additional note, due to the importance of the Docker Hub breach and the publicity it has received, it is plausible that threat actors use it for phishing attacks, crafting fake Docker password-change emails. Users should follow best practices on changing their passwords and not trust password change links in emails.