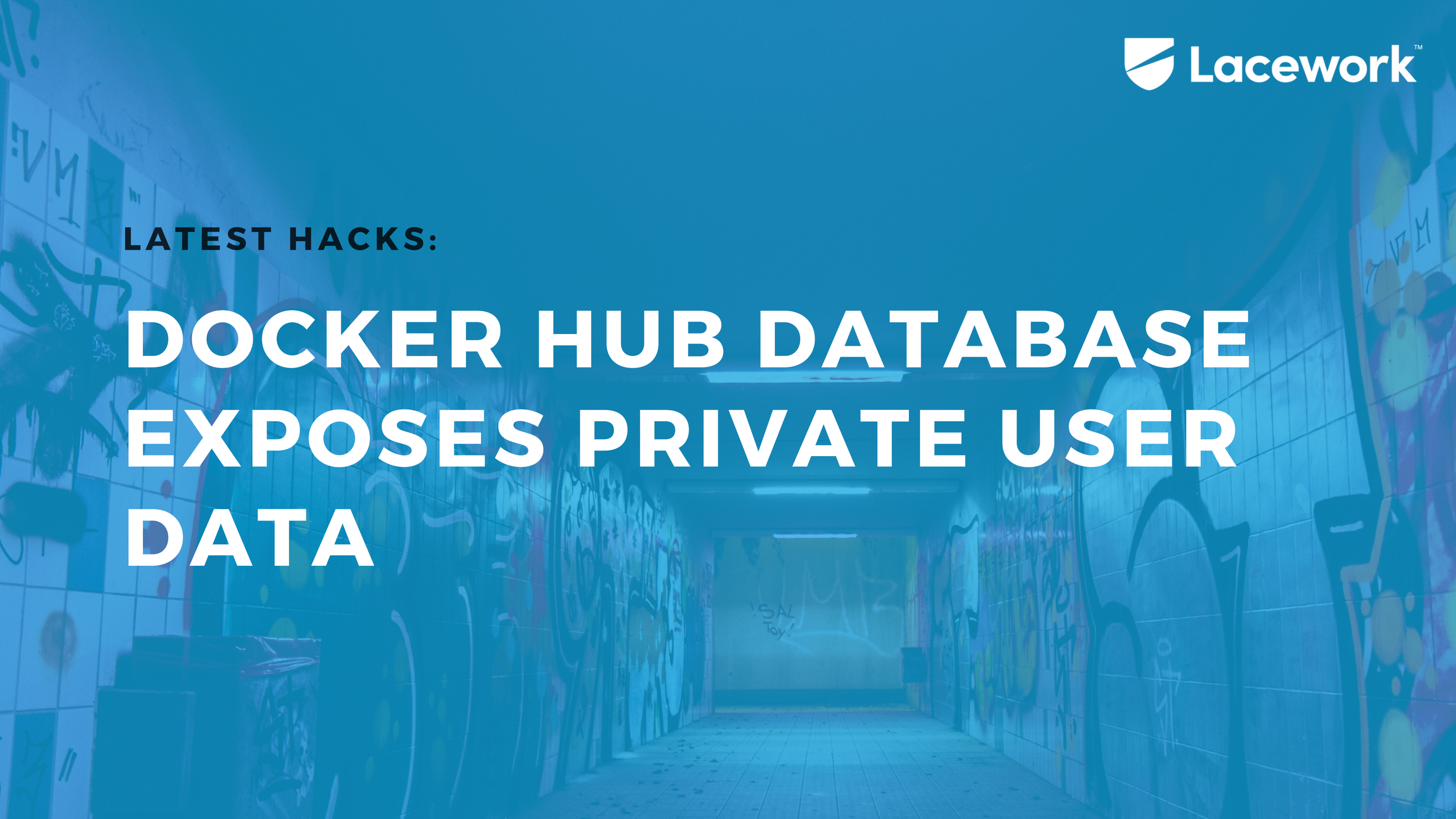


Lacework™

LATEST HACKS:

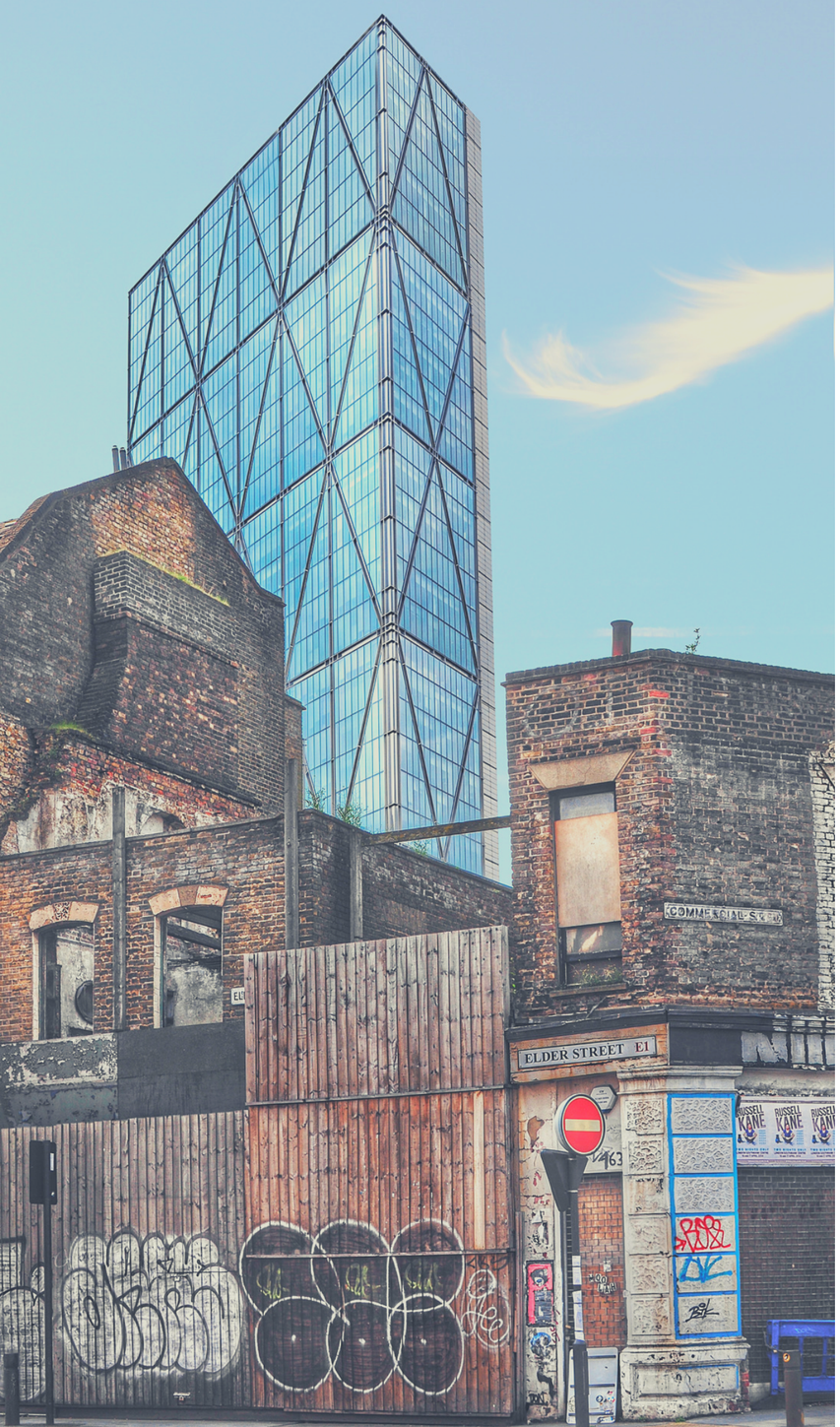
DOCKER HUB DATABASE EXPOSES PRIVATE USER DATA

OVERVIEW

A Docker Hub database that was not properly secured enabled an unauthorized user to gain access to sensitive information for 190,000 Docker users. The trove of data included usernames, passwords, and tokens for GitHub and Bitbucket autobuilds.

Based on what was extracted, it appears likely that the attackers had specific motives to get tokens and access keys that would enable them to access companies' private code repositories and potentially inject malicious code in auto-built containers. Some have speculated that even those who do not specifically use Docker Hub, but who have accessed Docker through GitHub integration.

Docker has stated that they have revoked all exposed tokens and access keys.



CAUSE

The attack is another case of credential compromise, and was likely not discovered because access rules may not have been compromised. In most cases, companies rely on rules-based systems to ensure things like access control. The problem is that impersonating a legitimate user is hard to detect through rules. It’s only through anomaly detection that security teams can accurately determine if abnormal behavior is occurring.

It’s likely that the attacker was extracting large amounts of data, or perhaps uncorrelated data, all of which could be detected through behavioral analysis. This approach looks at what’s specifically happening, and analyzes/evaluates that against normalized activity. In this approach, attackers can quickly be identified and issues isolated before they do more harm..

PREVENTION

Securing workloads in public clouds requires a different approach than that used for traditional data centers, where APIs drive the infrastructure and create short-lived workloads. In turn, they're also becoming more interesting to cybercriminals,

Hackers don't necessarily use complex coding skills for their attacks. As any experienced security professional can tell you, hackers mostly just want access; once in, they can extract data, initiate cryptomining, and deploy ransomware. The easiest way to gain that access is through impersonating a legitimate user, and because software cannot discern beyond valid credentials, it's critical that organizations have strong identify management policies.

Learn more about cloud security best practices.