



CUBBIT VAULT

-Deepak Mehra

About

Advanced online file encryption and decryption tool that helps user to encrypt files on client side, making it less vulnerable in the internet space and decreasing it's chances of getting viewed by third party.



Why should we care
about

“Client Side Encryption” ?



Users Data, belongs to the
CONSUMERS & “NOT” CORPORATES



pCloud



Dropbox



Google Drive



tresorit



sync.com

IDrive®



MEGA



OneDrive

box



MediaFire



SugarSync

CARBONITE™



zoolz

just cloud

6 Apple iCloud

Apple suffered what may be the largest high-profile cloud security breach involved. Jennifer Lawrence and other celebrities had their private photos of the victims initially thought that someone had hacked their individual [iCloud service](#) they used for personal storage had been compromised. Apple urged users to employ stronger passwords and introduced a notification system when suspicious account activity is detected.

April 25th: Docker Hub

Breach size: 190,000 accounts

Need: Container Visibility (HIDS)

CAUSE

Adopters of containerization were dealt a blow this year as the popular Docker Hub repository was compromised exposing 190,000 accounts. "On Thursday, April 25th, 2019, we discovered unauthorized access to a single Hub database storing a subset of non-financial user data," Kent Lamb, director of Docker Support, said in a [statement](#) posted to the Docker website. "Upon discovery, we acted quickly to intervene and secure the site."

The breach reached only 5% of Docker Hub customers, but it included compromise of tokens and access keys for autobuild functions in Github and Bitbucket. This gives the incident a possibility of bypassing authentication, possibly injecting malicious code into production pipelines of many companies, and perhaps also gaining copies of proprietary code. Given the gravity of this possibility, Docker made the unusual step of revoking these tokens before notifying customers. While some were upset by this disruption, others acknowledged the wisdom of rapidly removing the threat. Password reset notifications were also sent out to those affected.

Companies using Docker had to regenerate keys to spin their autobuild features back up. They also needed to trace back through log files to identify potential malicious activity. Docker did not reveal the cause of the breach, describing it only as "a brief period of unauthorized access." It can only be speculated that the attacker was able to get hold of credentials or exploit the servers involved. Meanwhile Docker customers are left with an uneasy realization that their containers could have been tampered with.

Activate Wind

2. Dropbox

No one knew the severity of the breach cloud-based file sharing giant [Dropbox](#) announced back in 2012. In fact, it wasn't until four years later that we learned what really happened. Hackers tapped into more than 68 million user accounts – email addresses and passwords included – representing nearly 5 gigabytes of data. But there's more! Those stolen credentials reportedly made their way to a dark web marketplace – the price for them was bitcoins. At the time, this was equivalent to roughly \$1,141. Dropbox responded by requesting a site-wide password reset from the user base. They also went into some generic spiel about its ongoing commitment to data security.

What Else ?

- 1) Direct exposure of data to service providers.
- 2) Cloud is secure, not the data stored in cloud.


AND THE WAR BEGINS...





Client Side Encryption

- 1) As an extra measure for personal security.
- 2) Client-side encryption seeks to eliminate the potential for data to be viewed by service providers.



Client-side encryption means that the **client** is **encrypting** the data and NOT sharing the key with the server. When done properly, this **would** prevent anyone without the key from deciphering the data.