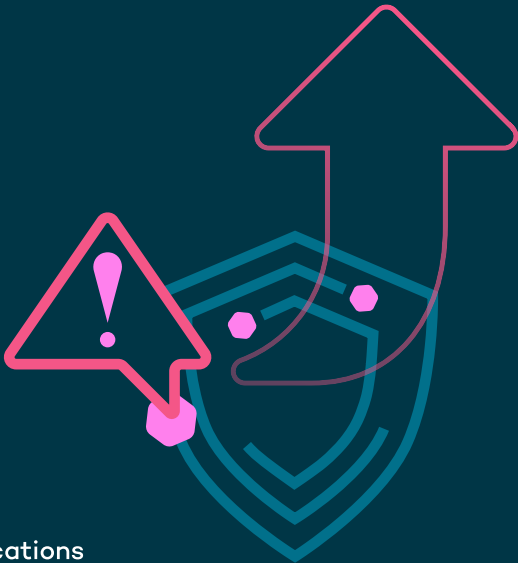





Major SaaS Security Breaches





Over the past two years, the SaaS mesh has exploded, with 1.5K applications and 900 integrations adopted by organizations on average—many of which are onboarded without security review. This has led to an increased frequency and magnitude of SaaS breaches and SaaS supply chain attacks. The following are some of the most destructive recent exploits.


**April 2022**




Attackers steal OAuth tokens from legitimate GitHub integrators







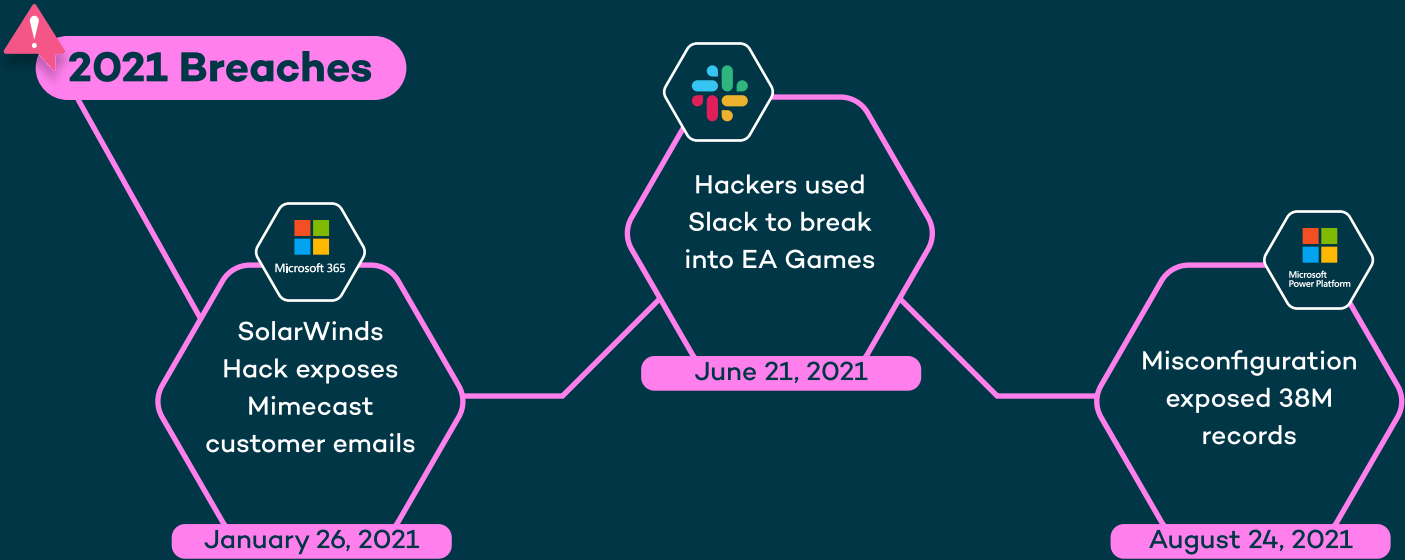
**GitHub**

Attackers abused the stolen OAuth tokens to access GitHub customer tenants

GitHub Attack Campaign

Attackers were able to steal and abuse OAuth tokens issued to well known vendors like Travis CI and Heroku.

The attackers were able to leverage the trust and high access granted to highly-reputed vendors to steal data from dozens of GitHub customers and private repositories.





Major SaaS Supply chain attacks and SaaS breaches are on the rise.

