- In July, 2023, Microsoft released blogs outlining a malicious campaign orchestrated by a nation-state adversary known as Storm-0558, which targeted customer emails within Microsoft environment. This successful breach was attributed to the authentication tokens, forged by the Threat Actor using potentially stolen Microsoft account (MSA) consumer signing keys. While significant discussions have arisen regarding the execution of this attack, many aspects remain shrouded in mystery. This presentation aims to dissect the attack, discussing both the confirmed details and the lingering uncertainties. We will delve into the vulnerabilities exploited by the adversary, analysing the gaps that facilitated the breach. Additionally, we will extract valuable insights from this incident, highlighting key lessons for organisations to fortify their defences against similar threats.