Email Bombing, Technique T1667 - Enterprise

Archived: 2026-04-05 15:08:21 UTC

Adversaries may flood targeted email addresses with an overwhelming volume of messages. This may bury legitimate emails in a flood of spam and disrupt business operations.[1][2]

An adversary may accomplish email bombing by leveraging an automated bot to register a targeted address for e-mail lists that do not validate new signups, such as online newsletters. The result can be a wave of thousands of e-mails that effectively overloads the victim's inbox.[2][3]

By sending hundreds or thousands of e-mails in quick succession, adversaries may successfully divert attention away from and bury legitimate messages including security alerts, daily business processes like help desk tickets and client correspondence, or ongoing scams.[3] This behavior can also be used as a tool of harassment.[2]

This behavior may be a precursor for Spearphishing Voice. For example, an adversary may email bomb a target and then follow up with a phone call to fraudulently offer assistance. This social engineering may lead to the use of Remote Access Software to steal credentials, deploy ransomware, conduct Financial Theft[1], or engage in other malicious activity.[4]

Source: https://attack.mitre.org/techniques/T1667